

Network Magazine

JUNE 2002

WHERE THE ENTERPRISE MEETS THE NEW PUBLIC NETWORK

Visionaries: *The Crystal Ball*



****AUTO**5-DIGIT 98073
#9028720432#NW514U
STEVE STROH
IND TECH WRITER
STEVE STROH
PO BOX 84
REDMOND WA 98073-0084

P119



Information is elusive. It changes every moment of every day. Information security requires the ability to control and adapt to any situation. Threats to information rely on old technologies that have remained stagnant long enough to be sidestepped. Often, packaged security solutions are obsolete before they are even applied.

Technology

go-red.com



SERVICES

PRODUCTS

TREND MICRO
CONTROL MANAGER

may guard information, but it is intelligence that makes it secure.

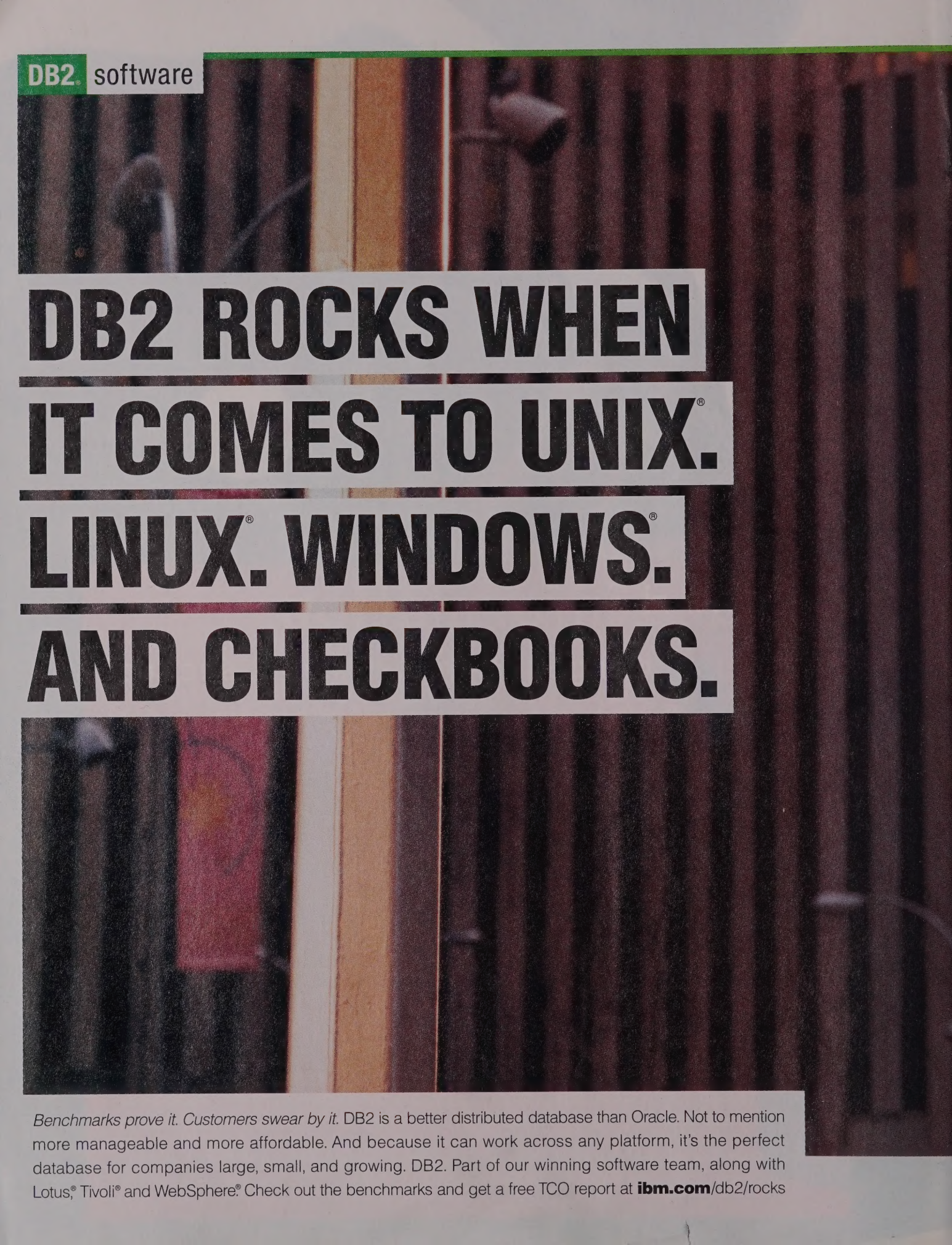
Intelligence comes from the ability to learn. But it is intuition — the application of knowledge based on experiences, patterns and trends — that allows intelligent strategies to be formed quickly. *Intuitive Information Security* uses innovative technology to deliver and adapt security strategies to the enterprise.

This is the idea behind *go-red*. It is the cumulative intelligence of hundreds, deployed by adaptive technology throughout the enterprise. Right down to the individual user, automatically, and in real time.

To understand how this may work, consider a virus outbreak. Every Trend Micro *Intuitive Information Security* strategy begins with TrendLabs. Made up of over 400 virus experts around the world, their collective intelligence is used to identify viruses, quickly develop isolation strategies and deploy them to the Control Manager software installed at the enterprise. Control Manager's technology then allows a set of policies to be automatically executed by any number of *go-red* information security products across the network. The result is a rapid and effective quarantine strategy.

During this time, TrendLabs works to break the code of the virus and establish a new strategy designed to eradicate the quarantined virus. Once this is accomplished, the strategy is again deployed via Control Manager, effectively cleaning the entire enterprise of any threat to its information.

Information will continue to change at a pace that packaged solutions cannot match. And although technology will continue to evolve, it is intelligence and intuition that will keep information secure.



DB2. software

DB2 ROCKS WHEN IT COMES TO UNIX.[®] LINUX.[®] WINDOWS.[®] AND CHECKBOOKS.

Benchmarks prove it. Customers swear by it. DB2 is a better distributed database than Oracle. Not to mention more manageable and more affordable. And because it can work across any platform, it's the perfect database for companies large, small, and growing. DB2. Part of our winning software team, along with Lotus,[®] Tivoli[®] and WebSphere.[®] Check out the benchmarks and get a free TCO report at **ibm.com/db2/rocks**

IBM, DB2, Lotus, Trivoli, WebSphere, the e-business logo and e-business is the game. Play to win are registered trademarks or trademarks of International Business Machines Corporation in the United States and/or other countries. Linux is a registered trademark of The Open Group in the United States and other countries. Windows is a registered trademark of Microsoft Corporation in the United States and/or other countries. © 2002 IBM Corporation. All rights reserved.

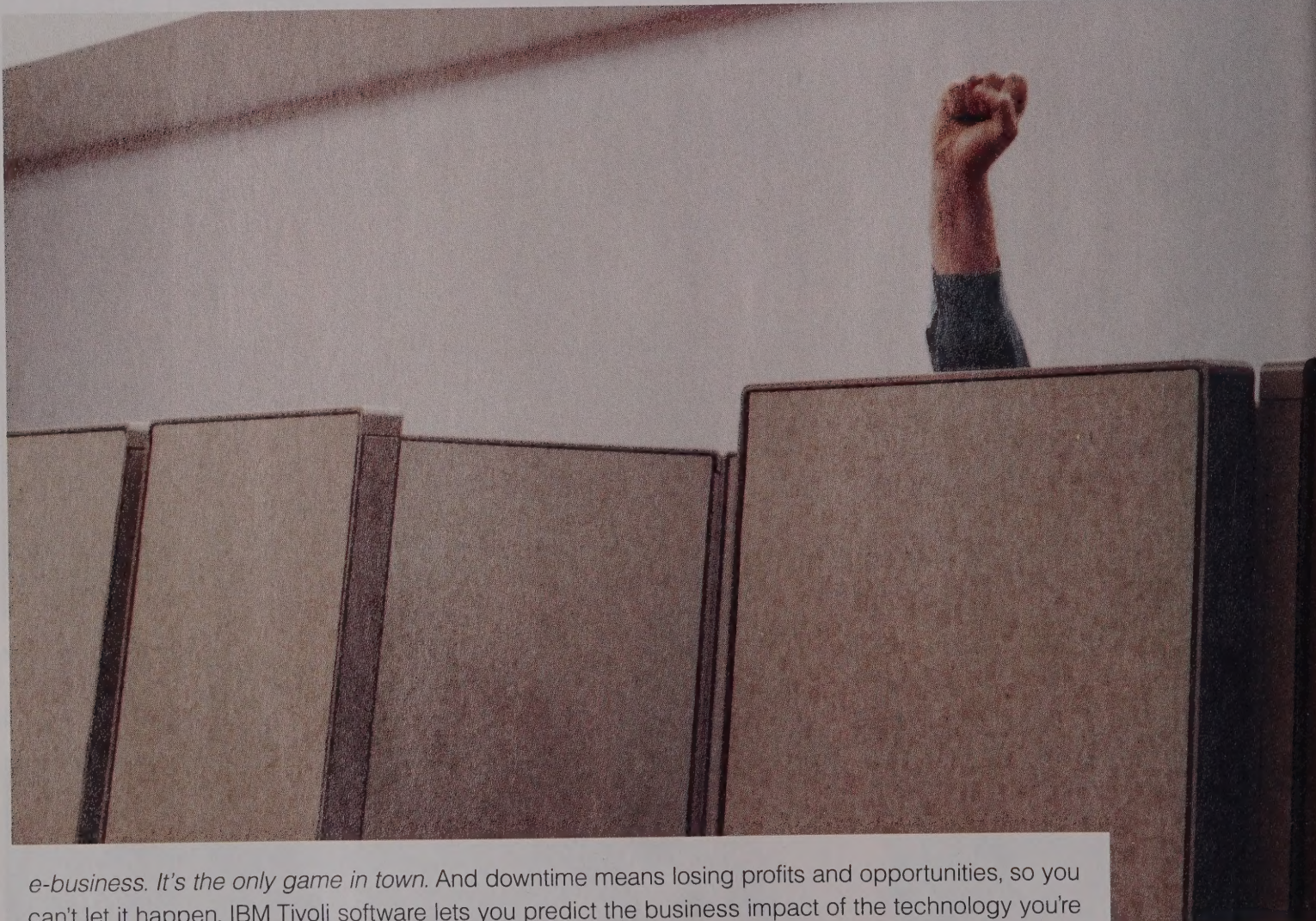


IBM®

e-business is the game. Play to win.™

Tivoli software

**IN THIS GAME, THERE
CAN BE NO TIMEOUTS.
NO DELAYS. NO STOPPAGE.**



e-business. It's the only game in town. And downtime means losing profits and opportunities, so you can't let it happen. IBM Tivoli software lets you predict the business impact of the technology you're responsible for, so that you can make smarter decisions today. Tivoli. Part of our winning software team, along with DB2®, Lotus® and WebSphere®. To find out more view our Webcast at ibm.com/tivoli/smarter

IBM, DB2, Lotus, Trivoli, WebSphere, the e-business logo, and e-business is the game. Play to win are registered trademarks or trademarks of International Business Machines Corporation in the United States and/or other countries. © 2002 IBM Corporation. All rights reserved.

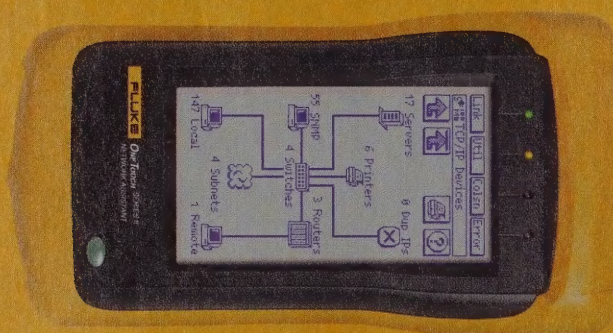


IBM

@business is the game. Play to win.™



NETWORK SUPERVISION™



The OneTouch™ Network Assistant gives your troubleshooting crews super human vision. Plug it into any port, press the AutoTest icon and the OneTouch eyeballs the entire network. Bingo: An instant read on the connectivity status of every desktop station, router, server and switch. Another touch zeros in on the exact switch port, printer or PC that's causing the problem. It checks everything from traffic snarls to NICs, hubs and cables. Problem solved. With OneTouch. One look and you'll want a OneTouch.

**See It.
Win It!**

See for yourself. Click into our live demo at www.fluke-net.com/1touch/ and enter to win a FREE OneTouch™ the fastest tool for first response troubleshooting.

©2001 Fluke Networks, Inc. U.S. (800) 283-5853. Canada (800) 363-5853.
Europe (31 40) 2 675 200. Other countries (425) 446-4519.
All rights reserved. www.flukenetworks.com Ad no. 01438

FLUKE
networks™

contents

Network Magazine

NPN NEW PUBLIC NETWORK

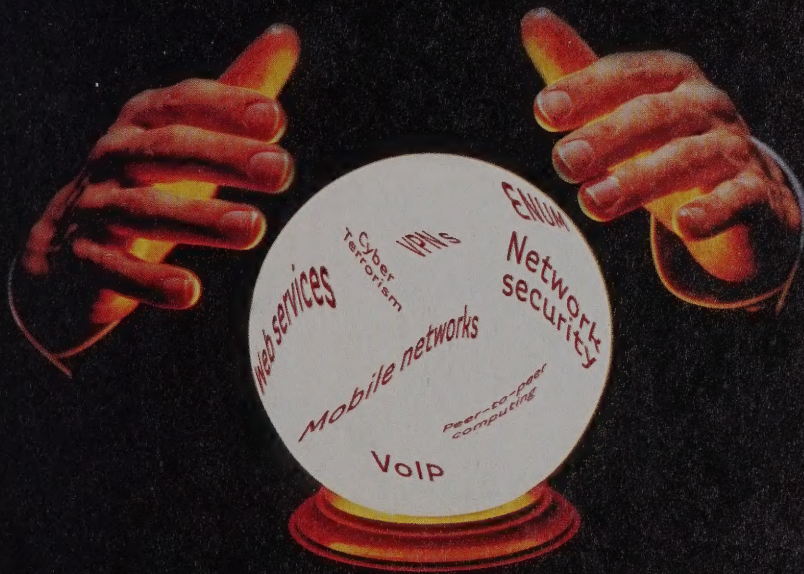
Crystal Ball Gazers

What does the future hold for networking?
We asked leading thinkers in the areas of carrier services, security, and Web services.

by David Greenfield

34

cover story



40

emerging technology

Convergence in the Enterprise: Does Anyone Care?

Apps that combine voice and data are starting to emerge. But do end users really want these features?

by Doug Allen



June 2002

Volume 17, Number 6

columns

80

The Business Layer

by Lenny Liebmann

Monitoring the End User.
The most critical component of the network doesn't have a MIB ... yet.

82

Network Defense

by Rik Farrow

VPN Vulnerabilities.
VPNs might be tunneling more through your firewall than you'd like.

86

Off the Wires

by Andy Dornan

How Vendors Use Math to Lie.
Optimists may have more fun, but pessimists are usually right.

104

Wide Angle

by Tom Nolle

Is Frame Forwarding
the Next Service Sensation?
MPLS-based services are exploding, but they're not always what they seem.

SUBSCRIPTION INFORMATION: One year (12 issues). U.S. & Canada: free to qualifying subscribers, or \$125. Mexico, South and Central America: \$180. Europe, Africa, Middle East, Asia/Pacific, and all others: \$160. For new orders and customer service in the U.S., call (800) 577-5356. International orders call (847) 647-6834.

POSTMASTER: Please send address changes to *Network Magazine*, P.O. Box 2013, Skokie, IL 60076. Allow six to eight weeks for subscription to begin. *Network Magazine* (ISSN 1093-8001) is published monthly by CMP Media LLC, 600 Community Drive, Manhasset, New York 11030. Periodicals postage paid at Manhasset, New York and additional mailing offices. Copyright © 2002, CMP Media LLC.

June
2002

Volume 17, Number 6

departments

10

Viewpoint

Reading Magazines

12

Letters

Making the Case for Cable.
MVNO Opportunities. Wireless Newbie
Inquires. Voicing Concern.

16

News

IP VPNs: Network-based, CPE, or both? Massive
Spam Increase Clogs Internet Arteries.
How Fast Can DAFS Make NAS?
Meridian VoIP Headaches.

24

Global Watch

Internet Governance.
Europe Warms to Hotspots.

28

Product Spotlight

OpenReach's Frame Relay Plus

30

Tutorial

Lesson 167:
Security and 802.11 Wireless Networks

78

New Products

Brocade Introduces New 2Gbit/sec Fibre
Channel Switch. GFI's MailSecurity Scans
E-Mail with Multiple Virus Engines.
AT&T Enhances VoIP Suite.

contents



Art, from left: Pep Montserrat, Victoria Kann, David Ball, Andrew Yates/Mercury Pictures

EMERGING TECHNOLOGY

Storage Networking: Fibre Channel, IP, and Beyond

How will Fibre Channel, IP, and emerging
interconnect technologies shape the new
networked storage landscape?

by Elizabeth Clark

46

PRODUCT FOCUS

Behavior-Blocking Stops Unknown Malicious Code

Behavior-blocking technology gives
administrators a leg up in the race
against zero-day exploits.

by Andrew Conry-Murray

50

EMERGING TECHNOLOGY

Ultra-Wideband Wireless: Fat Pipes from Thin Air?

UWB doesn't break the laws of physics,
but it's an exciting technology—and it
could even live up to Bluetooth's hype.

by Andy Dornan

67

BUSINESS CASE

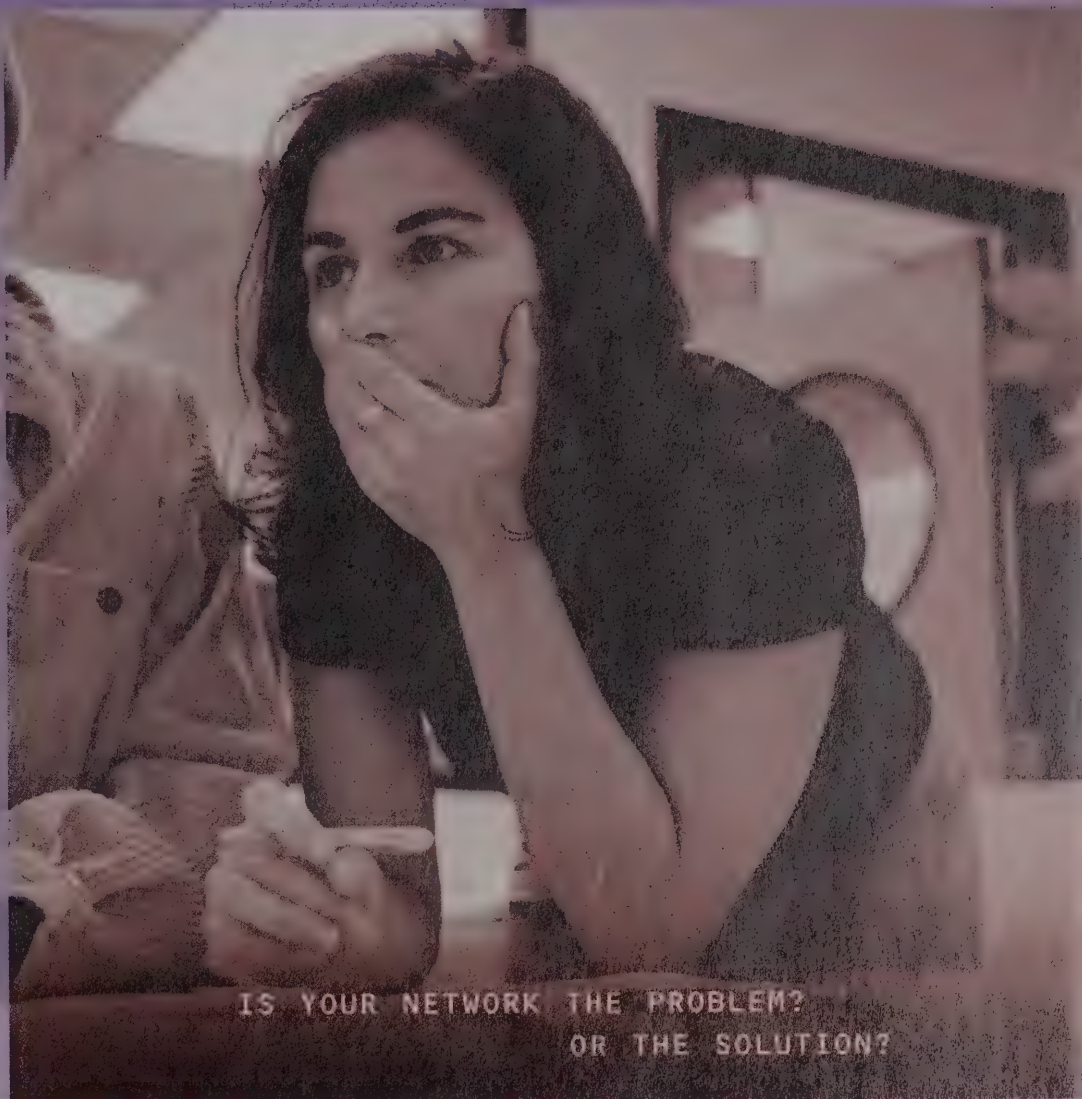
Hoover's Online Keeps Its Sub- scribers Online All Day, Every Day

Emerging from the dotcom shakeout
with profits, Hoover's Online ensures
24-by-7 uptime after deploying
application-tracking software.

by Jim Carr

72

- ▶ Authenticate and accelerate millions of SSL transactions with standard or FIPs certified security
- ▶ Update content and applications on global servers automatically
- ▶ Create an ECDN for security, reliability, scale and performance of applications
- ▶ Automatically route traffic via intelligent application and server load balancing
- ▶ Cache streaming media for better quality and speed at lower costs
- ▶ Centralize management for complete control of network and applications



IS YOUR NETWORK THE PROBLEM?
OR THE SOLUTION?



Mission critical? That's an understatement. eBusiness or enterprise, you depend on your network like never before. You need F5 like never before. Only F5 Networks — not any other company — gives you an end-to-end Internet traffic management and content delivery solution that is perfectly scalable, highly secure, remarkably integrated and ready for anything. Our open Internet Control Architecture, iControl™ platform/API and suite of award-winning products help you create the perfect application-aware network. And keep it under control. Find out why F5 is the leader. Visit www.f5.com or call 1-888-882-4447.



▶ CONTROL YOUR WORLD

Reading Magazines

From the beginning of the Internet Age, there have been widespread predictions of the impending death of media printed on paper. It's clear now that paper-based distribution and consumption of written, illustrated, and photographed material is no more likely to go away in the near term than is the paper-full office. Nevertheless, there are specific kinds of information I'm likely to read online instead of on paper.

The first variable I look at is length. I'm not comfortable reading anything more than a couple of pages long on a CRT or LCD display, but I might read dozens of onscreen short comments and responses on a discussion forum. A few research organizations prevent online readers from printing their reports, and I'll read these online if I'm sufficiently interested—even if they're 50 pages long (but I won't be comfortable at the end of the piece). In general, I'll print out all or at least the relevant parts of online documents that are over two pages long, particularly if they have multiple columns, which make online reading especially burdensome.

A lot of my work and personal activity is the result of e-mail, and I save e-mail messages that I'll need to refer to online, though I rarely print them. I see stacks of other people's printed e-mail on printers from time to time, and I wonder whether they're uncomfortable reading online media, or if they just find it easier to read printed material—even if it's short.

The second factor for me is timeliness. Something that matters to me right now, but won't need to be analyzed, documented, or consolidated with other material, is good online fodder. Political headlines, sports results, and market activity are typical examples. Logically, this would imply that daily and weekly publications would tend to work well online. Nevertheless, I read the San Francisco Chronicle and the New York Times for perhaps an hour most days, which seems to contradict the timeliness point. In fact, I can't imagine reading these newspapers online except for reference purposes. Part of the explanation is that I prefer reading longer articles (for example, the gory Enron details), opinion columns, and feature articles.



Over the years I've set up a handful of different filtering mechanisms—from Point-Cast to myYahoo to my.userland.com—to filter news that particularly interests me, but, invariably, these would yield too much stuff I didn't want to see, too little of the stuff I wanted to see, or both.

A handful of vendors, including one that *Network Magazine's* corporate masters have invested in, are proposing to deliver magazines to some subscribers electronically. (*Network Magazine* doesn't currently have plans to do such a thing.) The editorial content and the advertisements look just like the paper version. Some push mechanism—e-mail or other software—would automatically download the publication, and a subscriber could print

some or all of it. Unlike Web site content, these systems: 1) would not depend on subscriber initiative for downloading; 2) would not include back issues, discussion threads, news feeds, or reference material like Web sites do; and 3) would not have the redesigned look of a Web site. They would share some Web site properties, such as searchability by word.

Given the choice, there aren't many magazines I'd choose to get electronically. Most likely they would be those that I don't read in-depth. Portability is one problem—reading on the bus, in bed, or in the bathroom would mean either cranking up an unwieldy laptop, or printing out the content. Visual quality is another issue—certainly one of the reasons we get tired of reading on screens is that even high resolution monitors have nowhere near the resolution and contrast of good press-quality paper. When there's a lightweight, not-too-expensive tablet device with high resolution, high contrast, accurate color, a simple but powerful user interface, and room to store a few dozen magazines along with a handful of books, then I can imagine giving up paper magazines and books.

I'd like to hear about the factors that affect the choice of media for the things that you read. Are there other factors than length, timeliness, and portability that affect your decisions? *

Steve Steinke
Editor-in-Chief

Network Magazine

600 Harrison St., San Francisco, CA 94107
(415) 947-6360, Fax (415) 947-6022
www.networkmagazine.com

EDITORIAL

Editor-in-Chief

Steve Steinke ssteinke@cmp.com

Executive Editor

Elizabeth Clark eclark@cmp.com

Senior Editor

Doug Allen dallenz@cmp.com

Senior Editor

Andy Dornan adornan@cmp.com

International Technology Editor

David Greenfield dgreenfi@cmp.com

Business Editor

Andrew Conry-Murray amurray@cmp.com

Associate Editor

Rob Kirby rkirby@cmp.com

Associate Features Editor

Ellen Terry eterry@cmp.com

ART AND PRODUCTION

Managing Editor

Roger Burchill rburchill@cmp.com

Copy/Production Associate

Nancy Hung nhung@cmp.com

NETWORKMAGAZINE.COM

Webmaster

Todd Elkins telkins@cmp.com

CIRCULATION

Circulation Director

Dan Lenz dlencz@cmp.com

Circulation Fulfillment Manager

Pam Vandernoth pvandern@cmp.com

CUSTOMER SERVICE

U.S. (800) 577-5356 or International (847) 647-6834

Fax (847) 647-8648

www.networkmagazine@halldata.com

CMP Media LLC

President and CEO

Gary Marshall

Executive Vice President and CFO

John Day

President, Technology Solutions Group

Robert Faletra

President, Business Technology Group

Adam K. Marder

President, Healthcare Group

Vicki Masseria

President, Specialized Technologies Group

Regina Starr Ridley

President, Electronics Group

Steve Weitzner

Senior Vice President, Business Development

Vittoria Borazio

Senior Vice President, Global Sales and Marketing

Bill Howard

Senior Vice President,
Human Resources and Communications

Leah Landro

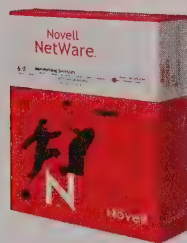
Vice President and General Counsel

Sandra Grayson



CMP

United Business Media



get NetWare 6.
now your **N**etwork
is just a browser away.

Need access from Australia? Want to print from Prague? Get the freedom of NetWare® 6. As part of Novell's one Net vision, NetWare 6 lets your users have access to their file, print and other storage resources from any browser in the world, anytime. So no more lugging laptops to Latin America. All they'll need is any computer with an Internet connection. That's it. And that's the beauty of one Net. So take this as a sign and visit www.novell.com/netware6 to learn more.

Novell
the power to chaNge™

Making the Case for Cable. MVNO Opportunities. Wireless Newbie Inquires. Voicing Concern.

MAKING THE CASE FOR CABLE

I read with great interest your commentary in "Are Cable Companies the Key to Local Access?" Wide Angle, April 2002, page 104). I work for a municipality in suburban Philadelphia, PA. We want to get Comcast's business cable Internet access. We met with a salesperson, and he even had a contract for us to look at to see what it involved. However when the tech people did their "site survey" (they never came to the site), they told us that we can't get the service because they don't have enough tech support.

Comcast bought out Adelphia Cable in our area a few years ago. Apparently, Comcast has been having a hard time training the Adelphia tech people on Comcast's equipment. We have no idea when we can get the service—nobody is telling the salesperson (at least that's what he says). It's offered five miles away in either direction, but not here. So we limp along with one very slow dial-up connection on one computer in somebody's office. Think good thoughts for us as we try to convince Comcast that we need them to give us the service now!

Dennis J. Blackburn

Thanks for your response. Residential customers of cable companies have complained of similar experiences when a new geography is opened up. Our local cable company used to run a commercial that said, in part, "When heaven was wired for cable...", and we didn't even have cable TV. I called them and quoted their ad, suggesting that they wire Voorhees before they did heaven. We got the cable.

One thing you might check is whether the service is offered on your cable span—the CATV that passes your business. If it's not, the problems might be formidable and

it might take some time to get them fixed. If it is, you might find that the reluctance of Comcast relates to how they could support a business customer. In that case, it might be that you could get a "residential" brand of the service. Be careful about their permitted use policy in that case. If you're not sure how to get a straight answer on what could be done, wait until you see a cable service truck and buy the driver lunch!

—Tom Nolle

Just wanted to say that I enjoyed "Are Cable Companies the Key to Local Access?" Your points about service were well directed. Of course, since our kids don't have the same history with cable service as we do I suppose they'll be less apt to care (at least initially) whom they get 1.5Mbps/sec from.

Aside from the investment in sales and service, cable may have a strategic advantage in that they can offer an array of broadband (including core business entertainment) services. The RBOCs aren't going to be able to deliver broadband to the home other than DSL. Even if they could deliver fiber options, the regulatory situation would force them to resell it—not good for return on investment. So I guess we're in for limited intermodal competition. Then, of course, there's the wireless wildcard...

Christopher Swann

Senior Consultant

DRI-WEFA

chris.swann@dri-wefa.com

Your summary of RBOC options is right on. Regulations have really shaped our set of options in the market, and I suspect the regulators had no idea what the impact would turn out to be. Ultimately, the war between RBOCs and cable may be decided by how well the dish people do; if cable margins on basic entertainment fall as fast or faster than legacy telephone service margins, the cable guys are squeezed. If it's the other way around, the RBOCs get squeezed.

—Tom Nolle

Regarding your opening paragraph in "Are Cable Companies the Key to Local Access?":

Quite a few years ago I asked one of the installers of phones in a New York office I worked in why they left a cardboard carton of quad wire just sitting there when they quit for the day. The guy replied that it was company policy (New York Telephone)—that way, someone who wanted some would take it from the carton, rather than pull it out of the wall.

My suspicion is that the same process might have been in place when you observed the neighborhood kids.

I'm not meaning to be critical. I enjoyed this article and many of your other ones for their healthy realism.

Jim Albert

Senior Project Manager

Danzas AEI

jim.albert@danzas.com

I agree! It sounds like the problem of kids dragging cable wire is endemic.

—Tom Nolle

MVNO OPPORTUNITIES

I enjoyed your article, "We Need Bandwidth, They Offer Brand Names," on Mobile Virtual Network Operators (MVNOs; Off the Wires, March 2002, page 78) very much and I'm going to order your book. We're a small company (a Competitive Local Exchange Carrier [CLEC]), and would like to know if you're aware of any MVNO/reseller opportunities available for smaller companies. Virgin is a very big company and I'm happy to see them "get in."

Gwen Joseph

advantell1@cox.net

There's no equivalent of "unbundling" in the mobile market, so MVNO opportunities depend on the policies of individual cellular operators. Some don't allow MVNOs at all (because their networks are already close to full capacity), while others will partner with smaller companies. Fixed-line telcos (including CLECs) do have an obvious advantage over other potential MVNOs in that they already sell telecom services, so they can offer integrated billing.

—Andy Dornan

WIRELESS NEWBIE INQUIRES

After reading "Emerging Technology: LANs with No Wires, but Strings Still Attached" (February 2002, page 44), I have

ERRATA

In "DHCP: Another Untrustworthy Service," Network Defense, April 2002, page 80, the Web site address for SysAdmin magazine was incorrectly noted. The correct address is www.sysadmin.com.



It's not just how we help millions of people worldwide avoid virus attacks.

It's how we help one customer with a problem.

That's the difference.

At Sophos, when one of our customers has a problem, we're there to help – whatever the size of the organization. We provide the best technical support in the business and our experts are on hand 24x7x365 to help our customers stay virus free. Of course, we also develop the world's leading anti-virus solution for corporate networks: a multi-platform defense which protects desktops, servers and email gateways.

1-800-779-9884
www.sophos.com

SOPHOS
ANTI-VIRUS

a question about network traffic and interference within the 2.4GHz range. If the 802.11b standard uses a frequency range equivalent to high-end cordless phones, how is data transmission affected? I know that the network speeds are slower, but will computers simply transmit/receive at a slower rate, or will PCs receive corrupted data? Also, how will the heavy traffic affect cordless phone conversations?

I appreciate your taking time to answer my questions. I am a "wireless newbie."

Levern Allen III

The only way to be sure is to test the individual devices. In general, people trying to use 802.11b and cordless phones together have found that they do still work, but with a reduced data rate and more dropped calls. However, how much they're affected also depends on other sources of interference, such as microwave ovens, Bluetooth devices, or wireless networks in neighboring buildings. Built-in error-correction should ensure that no data is corrupted.

—Andy Dornan

VOICING CONCERN

Your article "Just Say No to Voice Portals" (Off the Wires, February 2002, page 78) was a poor one at best. It's obvious that you don't know your speech recognition technology very well, mixing up the dictation-type software with the telephony-based type. You can buy the PC version for dictation for about \$100 from any software retail store, but the telephony-based software runs in the hundreds of dollars per telephone port and it works very well without individual voice training.

Studies conducted by Nuance Communications show that the accuracy rate over deployed telephony-based applications is well over 95 percent. I'm sure SpeechWorks, the other premier speech recognition vendor, has similar numbers.

You obviously think that the same software that runs on a desktop is also deployed in IVR [Interactive Voice Recognition] systems and that's where you are very, very wrong.

Also, keeping with your insistence to compare apples with oranges, you compare WAP [Wireless Application Protocol] with VoicexML [Extensible Markup Language]. Speech recognition can be programmed in a variety of languages of which VoicexML is (a standards-based) one. You can find folks programming speech recognition applications in C, Java, and other proprietary languages offered by all major IVR vendors.

You really need to get your facts straight before you shoot down an industry. You didn't do yourself any favors by writing this article.

Alex Mansour

alex.mansour@edify.com

Though IVR systems do use faster hardware and more expensive software than PC-based voice recognition, this isn't reflected in their performance: Improved accuracy is negated by the need to function over a telephone line. The figure of 95 percent is misleading. It refers to the success rate of an IVR system at recognizing a company name from a set of only 4,000, and was only achieved using a landline in a quiet environment. (The comparable figure for a hands-free car phone is only 89 percent.) More significantly, the tests allowed up to four attempts before a transaction was considered a failure. This means that one out of every 20 phrases couldn't be recognized, even after the computer had asked the customer to try again, and again, and again. I can't think of any other industries that would consider this something to boast about.

It's true that IVR systems can be programmed in a variety of languages, but so can mobile data devices. WAP and VoicexML aren't programming languages in the same sense as C: They're markup languages, designed to share data in a human-readable form. (The full WAP specification also includes some lower-level protocols in addition to the markup language, but these are now optional.) One advantage of using them is that, because they're based on XML, they make it easier to access data through a variety of different devices. If you're building an IVR system, basing it on VoicexML will help people to switch to a more reliable technology such as WAP when the voice recognition fails.

—Andy Dornan

PUBLISHER

Karla Johnson kjohnson@cmp.com
(212) 600-3067, Fax (212) 600-3175

ADVERTISING SALES

Southwest / Midwest 1 / Western Canada
Sales Executive
Jenny Gutierrez jgutierrez@cmp.com
(415) 947-6358, Fax (415) 947-6022

Northwest / Silicon Valley
Sales Executive
Jenny Gutierrez jgutierrez@cmp.com
(415) 947-6358, Fax (415) 947-6022

Northeast / Eastern Canada
Associate Publisher / Eastern Ad Sales Director
Amy Ventura aventura@cmp.com
(212) 600-3084, Fax (212) 600-3175

Southeast / Midwest 2
Sales Executive
Cara Capasso ccapasso@cmp.com
(212) 600-3024, Fax (212) 600-3175

Europe International Sales Representative
Michael Taylor mikelstay@aol.com
+44 1244 315695, Fax +44 1244 315695

Middle East / Italy
Independent Sales Representative, M@RS Marketing
Rhonda T. Abramson rhonda@actcom.co.il
+972 9 891 0611, Fax +972 9 891 0644

MARKETPLACE

National Sales Manager, Direct Response
Bethany Baller bballer@cmp.com
(716) 342-2484, Fax (716) 342-2488

NETWORKMAGAZINE.COM

Director of Content
Rick Luhmann rluhmann@cmp.com
(415) 947-6328, Fax (415) 947-6031

MARKETING AND CREATIVE DESIGN

Associate Publisher / Marketing Director
Amy Gamba Rouas agamba@cmp.com

Marketing Coordinator
Ann Freccero afreccero@cmp.com

Associate Design Director
Tim Haselman thaselman@cmp.com

ADVERTISING PRODUCTION

Production Supervisor
Stephanie Fung sfung@cmp.com
(415) 947-6607, Fax (415) 947-6079

REPRINTS

Stella Valdez svaldez@cmp.com
(916) 983-6971, Fax (916) 983-6972



CMP
United Business Media

LETTERS WELCOME

Network Magazine encourages letters from readers. Please tell us about your network-related problems—or solutions—and whether you agreed with, disagreed with, or didn't like an article. Include your name, company name, address, e-mail, and daytime telephone number. Here's how to reach us:

Letters to the Editor
Network Magazine
600 Harrison Street, San Francisco, CA 94107
Fax: (415) 947-6022
networkmag@cmp.com

We reserve the right to edit letters for space and clarity and to use them in our electronic and print editions (unless clearly marked "Not for Publication").

Are you future ready?

Solid Foundation for Your Network



"The most powerful, seamlessly adaptable systems of tomorrow invariably rely upon a solid foundation." Whether you are a service firm relying on your network to support your customers mission critical information or a technology manufacturer depending on your network to interface with suppliers, you share a common need for a reliable, long-term communication network infrastructure.

PANDUIT delivers solutions that help you maintain a reliable infrastructure and extend the life span of your network. Examples include Category 6 and Fiber Connectivity that exceed the most demanding industry performance standards, innovative designs that facilitate ease of proper installation and **modular solutions that support future system upgrades**. PANDUIT solutions combine to produce improved *installed* channel performance in support of your most demanding application requirements, now and into the future.

Be **FUTURE READY** with PANDUIT

PANDUIT is the Leading Global Provider of Network Connectivity Solutions

World-Leading Technology for Your Copper and Fiber Infrastructure

- **Connectors**
- **Outlets**
- **Network Interconnection Systems**
- **Raceway Systems**
- **Fiber Routing Systems**
- **Network Grounding Systems**
- **Network Cable Tie Systems**
- **Network Identification Systems**

World-Class Service

- **Worldwide Local Application Assistance**
- **Logistics Support—Worldwide Distributor Network**
- **Worldwide Warehouses and Manufacturing Facilities**
- **Worldwide Network of Design and Installation Companies**

To receive a copy of our Network Systems Catalog, please call

800-777-3300 or e-mail us at netconnsupport@panduit.com.

For technical assistance, call 866-405-6654.

CISCO SYSTEMS



Service Provider
Solution Partner



NETWORK CONNECTIVITY GROUP

Tinley Park, IL 60477

www.panduit.com/ncg/networkfoundation

News & Analysis



By the Numbers

12 Rank of the United States in a comparison of international broadband Internet penetration. South Korea is number one.

Source: Juniper Networks

10% Proportion of the poorest zip codes in the United States that don't have broadband Internet access available. In contrast, broadband is available in 96 percent of the richest zip codes. Source: Verizon

160,000 Number of broadband Internet connections in the United Kingdom, compared to 20 million phone lines.

Source: BT

98.8% Proportion of users of Japan's popular i-mode 9.6kbit/sec data service that haven't upgraded to third-generation (3G).

Source: NTT DoCoMo

IP VPNs: Network-based, CPE, or both?

Remember all the buzz about IP VPN services delivered from the network cloud? Back in the early days of 1999, IP Service Switches (IPSSs) from Shasta (now Nortel Networks), CoSine Communications, and SpringTide (now Lucent Technologies) promised to deliver value-added security services from the provider's edge.

The jury is still out on IPSSs. Providers such as SAVVIS Communications, Broadwing, and Qwest Communications have been successful in deploying them, but uptake has been slow, with customers numbering in the hundreds.

Vendors say the market needs more time to mature. But in the meantime, Multiservice Edge Router (MER) vendors such as Juniper Networks, Unisphere Networks, Laurel Networks, and Cisco Systems have taken advantage of the provider market's confusion by adding IP VPN technology to their boxes. These boxes sit at the network edge, but closer to the core than the customer premises or first provider POP. Unisphere has done particularly well in the edge aggregation space, focusing on layer-2 and layer-3 internetworking, so providers can run ATM and frame relay-enabled VPNs with Multiprotocol Label Switching (MPLS) for a slow, controlled migration to pure IP VPNs.

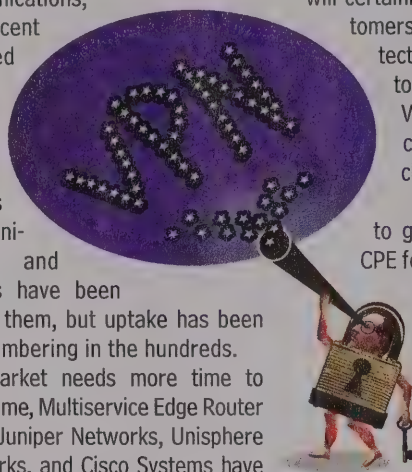
These MERs don't have all the value-added features, of, say, a CoSine box; most of the IPSS vendors plan to support tiered security services, such as network-based firewalls or intrusion detection. And despite the apparently strong showing of the MER market, many analysts see a gradual push over

the next few years to incorporate both IPSS and MER functionality in a single box, eliminating both categories as pure plays.

It appears that though network-based IP VPNs will certainly play a role in the future, business customers will have their pick of several VPN architectures. So the question really isn't whether to use network- or CPE-based gear for VPNs, but rather, which provider or vendor combination can provide the most flexible choices for deploying VPNs.

Analysts are divided about the best way to go. "Carriers are not good at managing CPE for customers," says Deb Mielke, principal of Treillage Network Strategies (www.treillagenetw.com). "Management systems don't scale, and there are all sorts of sparring, installation, software management, and inventory issues that are very hard to deal with."

Tom Nolle, president of CIMI Corp. (www.cimicorp.com), says, "I think network security is a real bad idea, like having terrorists do your security for you. The only kind of security that's reasonable is partitioned services such as frame relay, which don't create incremental security risks. Any form of encryption will either end up not really protecting you or will be compromised because you don't want the bother of key management... Even for a very small company, firewalling an Internet connection is relatively trivial, and the CPE is a hundred bucks. There's no business model to promote the survival of the providers that offer Internet tunneling. Could a carrier do anti-virus and firewall effectively? Not [if they want to] make money, which is all that counts." —Doug Allen, Boston



WHO'S HOT

Google wins a contract from America Online to be AOL's search engine of choice. Google, which displaces Inktomi and Overture, will provide both free and paid search services for the world's largest dial-up ISP.

Linksys Systems returns to its acquisitive ways as it snaps up a software company and ASIC maker for \$258 million in Cisco stock. The company hopes the acquired technology will give it a leg up in the router market.

Perot Systems raises nearly \$2 million in campaign funds during a stop in Silicon Valley. Apparently the tech sector hasn't run completely dry.

Daniel L. Smith, author of the Melissa virus, gets 20 months in jail, a \$5,000 fine, and is barred from using computers and the Internet for three years. Melissa ravaged e-mail systems in 1999 and cost millions in damage.

Thomas E. Ebbers resigns as WorldCom's president and CEO. Ebbers, who transformed WorldCom from an upstart long distance company into a telco powerhouse, was ousted due to a falling stock price and rising debt.

Sun Microsystems endures a rash of executive-level departures, including president and COO Ed Zander. Sun's share price dropped as a result.

WHO'S NOT



Illustration: Ben Fishman

Did you know you can
trade in your old APC units
for the latest and greatest
Single- and Three-phase
solutions? CALL TODAY!

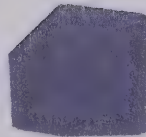
Respondents will receive APC's Solutions for
Business Networks brochure. Better yet, respond
today at the APC Web site!

<http://promo.apc.com> **Key Code**
f339y

(88) 289-APCC x6425 • FAX: (401) 788-2797

APC
Legendary Reliability™

Did you know you can trade in your old APC units for the
latest and greatest in Single- and Three-phase solutions?



☐ **YES!** Send me more information about APC Trade-UPS solutions. All respondents will receive APC's
Solutions for Business Networks brochure!

☐ **NO,** I'm not interested at this time, but please add me to your mailing list.

Name: _____ Title: _____

Company: _____

Address: _____ Address 2: _____

City/Town: _____ State: _____ Zip: _____ Country: _____

Phone: _____ Fax: _____ E-mail: _____

☐ **Yes!** Send me more information via e-mail and sign me up for APC PowerNews e-mail newsletter. **Key Code** f339y

What type of availability solution do you need?

- ☐ UPS: 0-16kVA (Single-phase) ☐ UPS: 10-80kVA (Three-phase AC) ☐ UPS: 80+ kVA (Three-phase AC) ☐ DC Power
☐ Network Enclosures and Racks ☐ Precision Air Conditioning ☐ Monitoring and Management ☐ Cables/Wires
☐ Mobile Protection ☐ Surge Protection ☐ UPS Upgrade ☐ Don't know

Purchase timeframe? ☐ < 1 Month ☐ 1-3 Months ☐ 3-12 Months ☐ 1 Yr. Plus ☐ Don't know

You are (check 1): ☐ Home/Home Office ☐ Business (<1000 employees) ☐ Large Corp. (>1000 employees)
☐ Gov't., Education, Public Org. ☐ APC Sellers & Partners



NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 36 WEST KINGSTON, RI

POSTAGE WILL BE PAID BY ADDRESSEE



KEY CODE: f339y
DEPARTMENT: C
132 FAIRGROUNDS ROAD
PO BOX 278
WEST KINGSTON RI 02892-9920



How to Contact APC

Call: (888) 289-APCC

use the extension on the reverse side

Fax: (401) 788-2797

Visit: <http://promo.apc.com>

use the key code on the reverse side



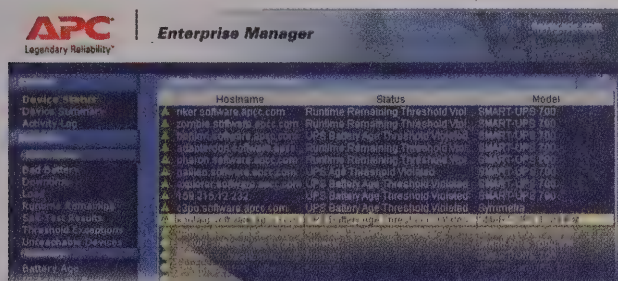
Now APC helps you solve your network's problems before they happen

Visit APC at
SUPERCOMM
Booth #11609

Can 10 Million Customers Be Wrong? Not About APC Smart-UPS®.

The world's most preferred server protection now comes with more intelligence.

APC Smart-UPS employ APC's PowerChute® Business Edition software to provide safe shutdown, power event analysis, recommended actions and mass configuration capability. Remote management is possible with APC's Web/SNMP Management Card.



For high-level network management, APC Enterprise Manager software is the answer. This scalable software allows management of hundreds or thousands of Smart-UPS simultaneously, regardless of how large an area they are distributed across.

APC's Smart-UPS range in size from 420VA to 5000VA and are perfect for protecting everything from small business servers to enterprise-level servers.

Contact APC today and let APC's Legendary Reliability™ work for you!



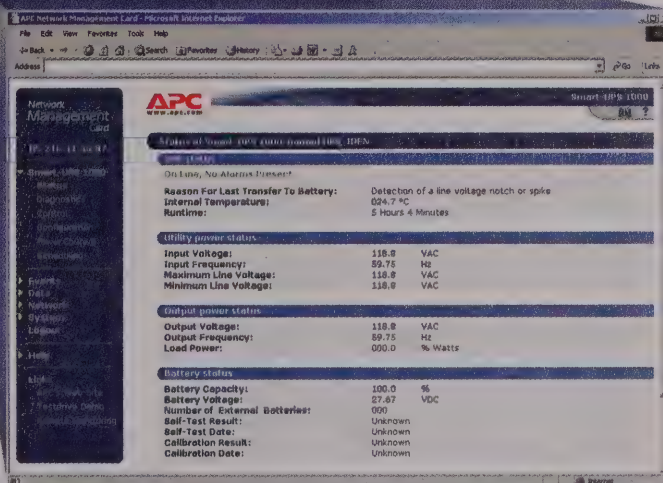
"APC UPS equipment is such an integral part of our network, it pays for itself every day."

Chris Michaels
Chief Technology Officer
Voyager.net [now dba CoreComm (www.corecomm.com)]

APC Enterprise Manager* Features:

- **Real-time Status and Event Notification:**
- Enables IT Managers to view status information for APC devices across the network at a glance and receive e-mail notification when there is a change in status
- **Recommended Actions:**
- Displays probable cause of power event and recommends a course of action to correct the problem, reducing the need for training and speeding troubleshooting
- **On-Demand Battery Status Reports:**
- Detailed reports on battery age, load, health, etc., facilitate the timely replacement of UPS batteries, reducing a major risk of downtime
- **Downtime and On-Battery Reports:**
- Unique reports help determine runtime throughout the network
- Helps network administrators to increase availability by pinpointing devices that require additional runtime and aids in Service Level Agreement management

Customize your Smart-UPS® with remote management and rebooting capabilities.



Smart-UPS® 1000 Tower
N+I 2001 "Best in Show"
Internet Week and
Network Computing

APC Smart-UPS® Features:

- **Improved Battery Management:**
Extended Range AVR Boost and Trim reduce battery usage
- **Multiple Communication Ports:**
Provide for USB and Serial connection
- **Built-in SmartSlot™:**
Lets you customize your Smart-UPS with remote management and rebooting capabilities, among other features
- **Improved, easier to read LED Display**
Display and alarms alert you to changes in battery and load conditions

APC
Legendary Reliability™

Also Look for Rack and Three-phase UPS Solutions from APC!

*Optional software for APC Smart-UPS. Not included.

Did you know you can trade in your old APC units for the latest and greatest in Single- and Three-phase solutions? CALL TODAY!

Visit <http://promo.apc.com> Key Code f339y or Call 888-289-APCC x6425 • Fax 401-788-2797

©2002 American Power Conversion. All Trademarks are the property of their owners. SU1A2EF-USB • PowerFax: (800) 347-FAXX • E-mail: esupport@apcc.com • 132 Fairgrounds Road, West Kingston, RI 02892 USA

Net Insights



MICHAEL KENNEDY
Co-founder
Network Strategy Partners
www.nspllc.com



JEFF PHILLIPS
Director
TeleChoice
www.telechoice.com

VPN Architecture Choices

This month on "As Our Telecom Market Turns," we focus on the less than stellar progress of IP Service Switches (IPSSs), widely touted from 1999 to 2001 as the ideal way to deliver security services. These IPSSs reside at the network edge instead of the customer premises, saving the carrier valuable capex and opex dollars and freeing customer IT staff from nasty management chores. However, end-user needs aren't quite simple enough for an either/or solution, as seen below.

Michael Kennedy is co-founder of Network Strategy Partners (www.nspllc.com), a consultancy firm. Jeff Phillips is the director of TeleChoice (www.telechoice.com).

1. How would you evaluate the validity of IPSS based on field deployments thus far?

Michael Kennedy I think the slow start should be viewed as discouraging. Movement is very slow. IP VPN seems to be slowly evolving as a replacement for corporate Remote Access Services [RAS], and traditional solutions such as frame relay Permanent Virtual Circuits [PVCs] tied to customer-owned and -operated routers have a lot of staying power. Thus, a market window is closing. It seems likely that by the time network-based services are widely accepted, a new generation of devices will come into the market to capture the big profits. IPSS is an all-or-nothing proposition. It's best for big mass-market solutions, but those are the hardest to develop.

Jeff Phillips I think most of the early wins were based on a big access line aggregation play, as opposed to IP VPN services. Today, and in the short term, IPSS will play really nice into mass-market security solutions such as small and medium-sized business [SMB], broadband, remote or off-network sites of enterprises. They also play nicely for static "private" networks of large enterprises. It's just another, more secure, way to deliver point-to-point

connections but do it via IP and Multiprotocol Label Switching [MPLS], IPSec, or both.

2. Given that the network-based IP services market is still evolving, with functionality spread out across different devices, what impact will this have on the enterprise end user's IP VPN and security setup?

Michael Kennedy I think we're likely to see many hybrid scenarios. Large enterprises are very unlikely to give up customer-premises-located firewalls for their large locations. However, it just isn't practical to place equipment in all of the places [home offices, alliance partners, and so on] that they now must support. I think network-based solutions have a good opportunity, especially for extending enterprise networks into the consumer broadband [work-at-home] marketplace.

Jeff Phillips End users are still partial to Customer Premises Equipment [CPE] and still partial to doing it themselves vs. outsourcing. Carriers will continue to look for ways to make it more attractive to outsource, and so have to be able to support a wide range of enterprise needs and do it as efficiently as they can where they

can. At the same time, edge gear, such as IPSSs and Multiservice Edge Routers [MERs], will continue to collapse things, which will impact CPE gear deployments. The IPSS is one way you'll see other security apps delivered from the cloud, but I think long term the VPN is moving further into the enterprise than it is into the cloud.

3. If you were advising customers on how to evaluate an IP VPN solution—network-based vs. CPE—which criteria would you have them focus on?

Michael Kennedy I would recommend that the small, closed network stay with the CPE solution, and that the network that involves lots of partners and work-at-home road-warriors and so on, go the network-based route whenever possible.

Jeff Phillips I'd evaluate the customers' security requirements, cost constraints, in-house expertise, and the level of control/customization they require. (Anything you customize eventually becomes your legacy stuff.) The bigger issue, though, is that any type of box still doesn't deliver on the "virtual" part of VPN: The hardware costs a bunch of money and will be obsolete one day.

Massive Spam Increase Clogs Internet Arteries

Nearly 20 percent of e-mail traffic is spam, according to Francois Lavaste, vice president of marketing at Brightmail (www.brightmail.com), a company that provides anti-spam, anti-virus, and content filtering services.

In just one year's time, the company has seen the number of spam attacks increase fivefold: from just over 680,000 in March 2001 to more than 3.7 million in March 2002 (see "The Pulse," page 20). Brightmail categorizes a spam attack as a mass mailing of a spam message, not a single mailing.

Lavaste attributes this surge to three factors. The first may be the unintended consequence of attempts to discourage spammers. For several years, e-mail users have been urged not to reply to spam. That's because any response—even a request to be removed from a mailing list—tells the spammer your account is valid. The theory was that spam would dry up if people stopped responding.

Unfortunately, this method appears to have had the opposite effect. "If

you're a spammer, and your response rate goes down, the answer is to spam more people, not stop spamming," says Lavaste. Once a spammer has invested the time and resources to set up shop, sending two million e-mails a day is just as easy as sending one million.

Second, Lavaste says that in today's sagging economy, more people may be turning to spam in an attempt to earn extra money. Third, sophisticated but easy-to-use mailing tools can transform anyone with half a brain and a PC into a spamming titan.

To combat this rise in unwanted e-mail, many individuals and organizations are turning to the law. Eighteen states have anti-spam legislation on the books, and many spammers have been penalized. For instance, in spring 2002 a nonprofit organization in Washington won \$3,000 in small-claims suits against three spammers. Anti-spam activists hope successful cases like this will encourage more suits, thus making spam less attractive to would-be entrepreneurs. —Andrew Conry-Murray, San Francisco



Cutting, squeezing and overhauling

budgets have always been the toughest part of your job. But you now find those skills being tested like never before when challenged to reduce infrastructure costs without risking your long-term business objectives.

HP Services can help: thousands of infrastructure specialists who have provided IT operations for hundreds of companies around the world. People who work with you to address virtually every aspect of your infrastructure. From streamlining operations to reducing overhead to simplifying processes. All while ensuring that the solution is flexible enough to evolve with your changing needs.

That's because our outsourcing solutions always start with you—your issues, your people, your challenges. So we can take on entire operations or parts of operations depending on the specific business goals you hope to achieve.

HP infrastructure solutions are engineered for the real world of business. Because the last time we checked, that's where we all work. Call 1.800.HPASKME, ext. 246. Or visit www.hp.com/go/infrastructure.

Infrastructure: it starts with you.





Spam on the Rise

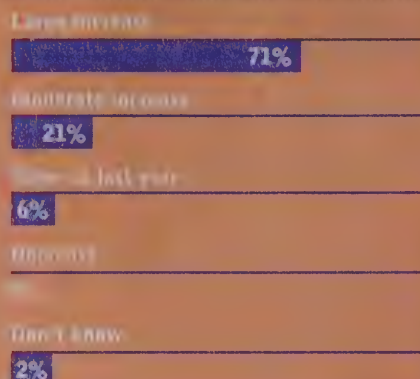
The amount of spam clogging corporate in-boxes has risen five-fold in the past year, according to anti-spam service provider Brightmail. The company measures junk mail via hundreds of thousands of dummy e-mail accounts planted throughout the Internet. Our online survey asked readers if they were being flooded by spam and requested that they tell us the steps they're taking to beat back the tide of bulk e-mail.

"The vast majority of my spam mail is pornographic in nature and I am transitioning away from my AOL account where it is most prevalent. It has now begun to creep into my corporate account which is of great concern to me."

"I believe that spammers should be required by law to be more responsive to "unsubscribe" requests. I find these request are more frequently ignored than ignored."

"This poll is skewed towards making one hate spam. I don't mind receiving great offers that I may never know about. Really, how difficult is it to hit a delete button? I would rather receive 50 emails that I can instantly delete than three cold calls to my house at night."

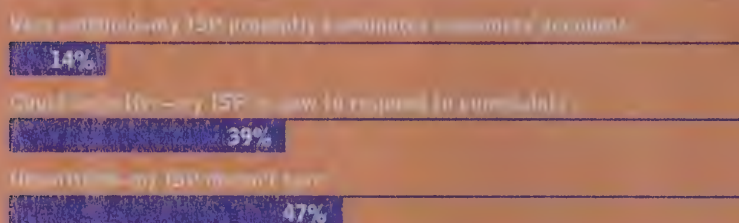
Has the amount of spam hitting your e-mail servers increased in the last year?



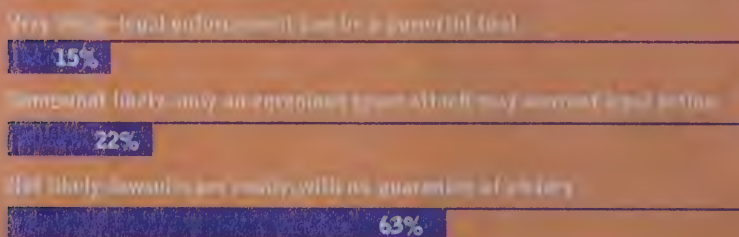
How often do you report spammers to your ISP?



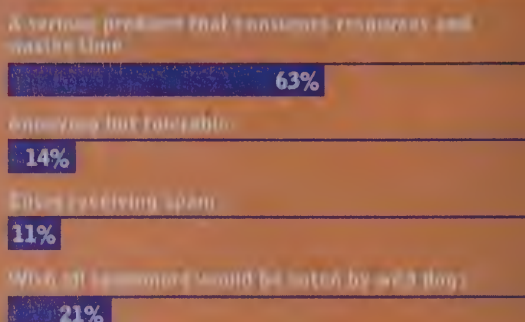
Are you satisfied with how your ISP deals with spammers?



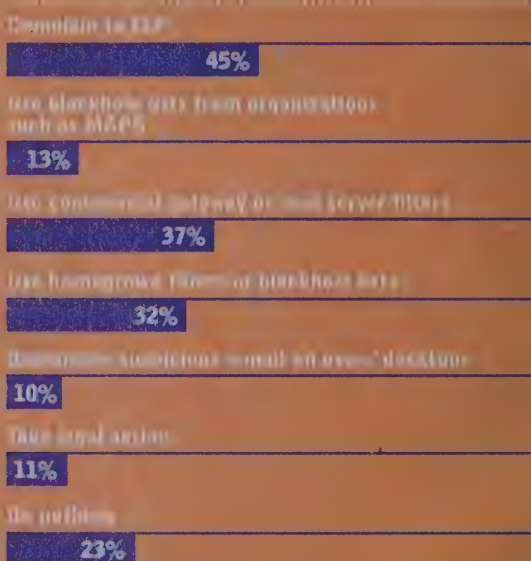
Eighteen states now have anti-spam laws on the books. How inclined are you to take a spammer to court?



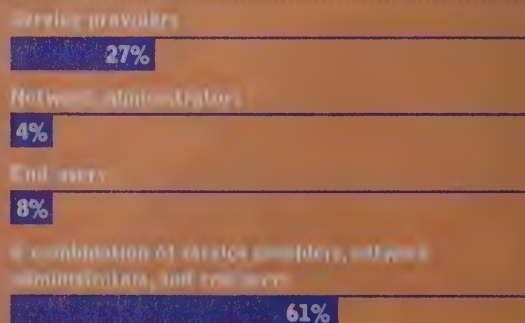
What is your attitude toward spam?

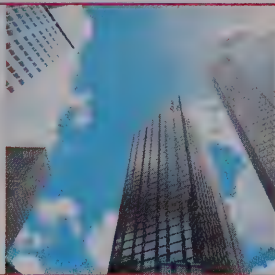


Have you taken any spam countermeasures? (Multiple responses accepted.)



Who should be responsible for dealing with spam?





YOU'RE PUTTING UP A

MULTI-MILLION-DOLLAR

OFFICE COMPLEX.

THIS IS NO TIME TO

CUT CORNERS ON

NETWORK INSTALLATION.

If you think cheap labor is a good idea,
you could be making an expensive mistake.

Networks can have problems. About 50% of
the time, they can be traced to the structured
cabling installation. How can you minimize the
effect of these problems? Hire a contractor
who employs a workforce that has been
well-trained, one that is qualified and takes
pride in a job done right.

The NECA-IBEW team has trained such
a workforce. IBEW electricians and
telecommunications technicians and installers
have the high-quality skills you need.

Not sure? Don't find out the hard way—
hire a NECA-IBEW contractor for your next
project and get it done right, the first time.

www.necanet.org





Standards Spotlight

Four Standards Out of the Blue

The Bluetooth specification for wireless Personal Area Networks (PANs) hasn't yet been as successful as its founders hoped. One reason is that, though often touted as a standard, it's really a proprietary system from an alliance of vendors, the Bluetooth Special Interest Group (SIG, at www.bluetooth.com). This is a large group that almost anyone can join—it had over 2,500 members at the last count—but it's ultimately dominated by the large cell phone manufacturers.

The IEEE is trying to boost the adoption of wireless PANs with its own standard, 802.15. This isn't exactly a rival to Bluetooth, because the two are almost identical. The first version of the standard, IEEE 802.15.1, was approved in April 2002, and is fully backwards-compatible with Bluetooth. Like its proprietary predecessor, it uses Frequency-Hopping Spread Spectrum (FHSS) to achieve a data rate of about 700Kbits/sec over a distance of up to 10 meters.

In the long term, the 802.15 working group wants to do more than simply standardize Bluetooth. It's working on three new versions, for different applications:

802.15.2 will offer similar abilities to those of Bluetooth and 802.15.1, but is designed to coexist with 802.11b (Wi-Fi) Wireless LANs (WLANs) without causing interference.

802.15.3 aims to increase the data rate. The target was originally 20Mbits/sec, but some prototypes are already achieving five times this. (See "Ultra-Wideband Wireless: Fat Pipes from Thin Air?," page 67.)

802.15.4 is a low power version, with a low data rate and long battery life. It's intended for smart cards, security tags, and other embedded devices. —Andy Dornan, San Francisco

How Fast Can DAFS Make NAS?

For years, Storage Area Network (SAN) fans have labeled Network Attached Storage (NAS) as too low-octane for high-performance applications. But the long-awaited Direct Access File System (DAFS) may be the tune-up NAS needs to help close the performance gap with SANs.

Initially developed by the DAFS Collaborative, founded by Network Appliance (www.netapp.com) and Intel, DAFS is a file access protocol that holds the promise of lower-latency, higher-throughput data transfers for NAS systems.

DAFS represents an improvement over the predominant protocols—Network File System (NFS) and Common Internet File System (CIFS)—which are based on technologies devised in the 1980s.

DAFS is based on a direct memory-to-memory architecture, and can run on interconnects that support the Virtual Interface (VI), which is optimized for use in server clusters. DAFS can run on Fibre Channel, Gigabit Ethernet, and an emerging interconnect technology called InfiniBand.

Just how far will DAFS go? Well, it's now an IETF Internet-Draft. And Network Appliance recently introduced the first DAFS-based product, the DAFS Database Accelerator, designed to boost the performance of Oracle, DB2, and Sybase applications running on its F800 filers.

Randy Kerns, senior partner with the Evaluator Group (www.evaluatorgroup.com), a storage analysis firm, is bullish on the protocol. "It's going to change everything," he says, "because it will allow you to [handle] transaction processing and databases in an exceptionally fast manner that was not possible before."

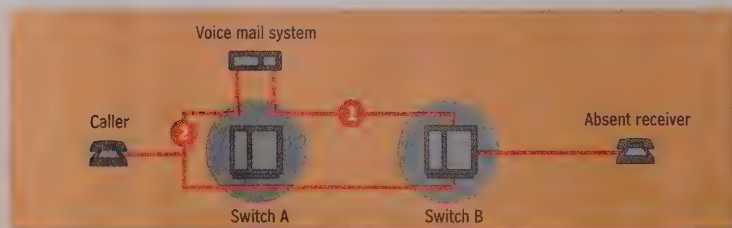
Curtis Preston, president of storage consulting firm The Storage Group (www.thestoragegroup.com), concurs that DAFS is a promising approach for enhancing performance, but says widespread adoption will hinge on many factors. One of these is whether DAFS will be as easy to use as NFS and CIFS. In addition, says Preston, "The Unix and Windows vendors will have to put DAFS clients into their OS—and that's going to take years."

—Elizabeth Clark, Atlanta

Meridian VoIP Headaches

A problem in Nortel's Meridian phone switches may deter companies from transiting to Voice over IP (VoIP) networks. The problem, called tromboning in Nortel parlance, occurs when PBXs transfer calls between sites. The Meridian establishes an additional call-path to the new destination instead of instructing the originating PBX to contact the new destination directly (see figure). As a result, latency and encoding are doubled, degrading voice quality.

"As soon as a transfer or redirection occurs, the quality degrades,"



Brassed Off. With tromboning, a return call path from switch B is used to direct a missed call back to the voice mail system (1), increasing latency and encoding and decreasing voice quality. Switches with anti-tromboning measures drop the original call path and direct the caller directly to the voice mail system (2).

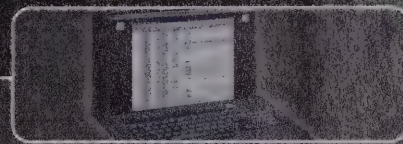
explains Scott Magerfleisch, a senior voice network analyst at a major financial institution, "The more times the call is transferred, the worse the voice quality."

Nortel has a solution for tromboning, but the solution doesn't work with its ITG2 Trunk Card, which enables the Meridians to communicate via an IP network. This is despite a new release of the Meridian code (Release 25).

Magerfleisch, who runs a 70-site frame relay network, hoped to use the network's excess capacity for the additional voice traffic. With each site equipped with a Meridian PBX, equipping the switches with the ITG2 made the most sense. There would be nominal impact on the hardware and no changes to the user interface or voice-support procedures, he says. Although Nortel offers other products that address the tromboning over IP issue, Magerfleisch is waiting to deploy VoIP until the company finds a better solution.

Meanwhile, users of Meridian competitor Avaya's Definity switch won't encounter the same problem. Avaya provides a number of techniques to address tromboning, or "hair pinning and shuffling" in Avaya's parlance, says Elliot Zeltzer, manager of telecommunications and network services at Gedas USA (www.gedas.com), a leading systems integrator in the automotive and manufacturing sectors and a Definity user. —David Greenfield, Jerusalem

THAT SENSATION OF TREMENDOUS SPEED IS BROUGHT TO YOU BY FINISAR.



Power. Precision. Protocol Analysis.

Increasing the speed of your network is at the core of what Finisar has been offering its customers for over 14 years. Finisar's family of network analysis and performance testing products ensure optimum performance through constant monitoring, measuring and analyzing to locate problems and fix them before they impact your company.

We listen to our customers, creating products that are flexible and scalable to grow and evolve with your needs along with the requirements of LAN to SAN. No other company offers products as easy-to-use and easy-to-implement.

Are you ready to run your network at full speed?

Finisar



The *ultimate* in SAN LAN performance tools.

www.gofinisar.com

1-888-746-6484

REGIONS & REGULATIONS

SPAIN

Snip, snip. That's the sound of Telefonica cutting local loop rates charged to rivals. The local regulator ordered the incumbent to cut prices on more than 50 services, causing a reduction of 50 percent or more. The move came in response to complaints from two smaller operators, Lince Telecomunicaciones and Alo Comunicaciones, charging that Telefonica missed deadlines and dragged its feet (or wires, as the case may be) to prevent connecting them to its network.

SWITZERLAND

No more middle-aged telecoms for this country. The government decided last April to open up the local loop and bring some much needed competition into Switzerland. Under the plan, the government aims to unbundle the local loop, and possibly the cable infrastructure. At press time, Swisscom was planning to fight the decision in the country's highest court.

FRANCE

The French regulator is following suit with new pricing for unbundled access. The new tariff cuts access rates by 28 percent, down to 10.5 Euros, or about U.S. \$9.50. The aim is to encourage unbundling beyond the major businesses in the largest towns. France Telecom will also have to offer competitors colocation space in the same room as the incumbent's gear if no other space is available, provide unaccompanied access to equipment in the colocation space, and offer installation deadlines.

Internet Governance

When Stuart Lynn came out of retirement to take over as president of the Internet Corporation for Assigned Names and Numbers (ICANN, www.icann.org) in March 2001, he knew his job would be tough, he just didn't know how tough. ICANN was to be the organization that brought private sector, Internet-speed thinking to administrative and policy management of the Internet's naming and address allocation systems.

And ICANN did experience some success. It created seven new Top Level Domains (TLDs), initiated a competitive registration process that changed TLD pricing and packaging, and formed a Uniform Dispute Resolution Policy for helping companies resolve domain name disputes.

But virtual idealism gave way to classic organizational challenges. Process, not substance, dominated ICANN, making implementation of strategic technologies, such as Electronic Numbering (ENUM), questionable. The lack of formal, stable relationships with registries for the country code TLDs (ccTLDs) posed a long-term risk to the Internet's global interoperability. Without the active participation of international governments, ICANN's effectiveness was limited. In short, ICANN couldn't effectively fulfill its mission under the current conditions.

What ICANN needed was a shakeup, something for which Lynn was uniquely equipped. An award-winning amateur photographer whose specialty lies in montages of digital images, the 63-year-old CEO would need all of his talents to blend the contributions of voracious Internet advocates. Lynn issued his call to arms in February 2002 with a 38-page report outlining his charge for ICANN and asking for input from the Internet community. Five months and over 100 comments later, Lynn will present his recommendations at

ICANN's next conference in Bucharest.

What should people expect to learn? According to Joe Sims, outside counsel for ICANN, funding will be a hot area. ICANN today runs on a \$5 million budget, and though it anticipates a 20-person staff, currently only 14 people are hired. One suggestion will be to gain funding by taking a small piece of name registration fees. Networkers should not get too worried, says Sims, as pennies, not dollars, are being talked about as the fee.

There has also been a lot of discussion around policy development. Currently, there's no clear deadline for policies to be developed—discussions drag on for months, not weeks. There needs to be a consensus for a time table during which problems are resolved, and a clear structure for processing new ideas. Of course, the details of how to run that process are critical. Although Sims wouldn't tip Lynn's hand, he acknowledges that the process needs to be conducted in a way that doesn't disenfranchise anyone. "One idea is to self-organize into forums or constituencies," he says, "This will be the vehicle in which things are made known on different matters."

Lynn will also likely talk about a process for selecting board members. There appears to be a developing consensus that ICANN needs qualified people who aren't necessarily technical experts, and some form of process for nominating them, says Sims. As for international cooperation of ccTLDs, Sims sees their participation as an outgrowth of those efforts.

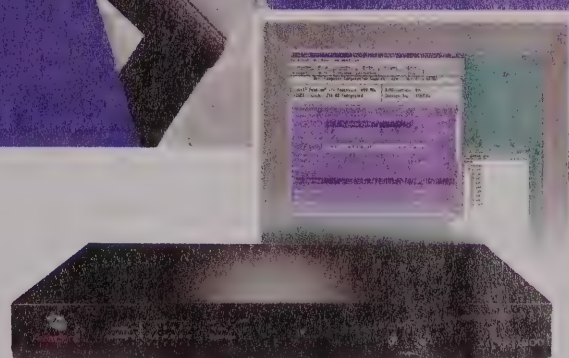
If Lynn is effective in his reorganization, he'll lead ICANN to the next stage of assuming responsibility for managing the "A" root servers of DNS—the spine of the Internet. Maybe then this beleaguered Internet organization will let its 63-year-old CEO return to retirement, but that's not very likely.

—David Greenfield, Jerusalem

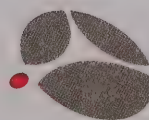


Is Your KVM Switch

Missing Something?



DS Series switches give you point and click access to all devices in your data center.



Avocent™

The Power of Being There™

Only Avocent KVM Switches give you a complete solution for secure access and control of your data center devices. Troubleshoot and control your servers, as well as routers, hubs, power distribution units and other serial devices. With KVM OVER IP™ and dedicated analog access, you can quickly control any of your data center devices from any location you choose.

Take your data center to the next step. Find out how you can centralize control and maintain network security. Download your free KVM Tech Guide at www.avocent.com/kvmguide or call **1-866-286-2368**.

Tariff Tracker

o the homework and negotiate. That should be the mantra of anybody serious about purchasing leased circuits in Europe these days. Until the days of competition, the incumbent's tariff represented the rate at which customers could buy services. Today's competitive markets mean that, "In many cases, tariffs are not relevant while market rates are very relevant," says Thomas Bookwalter, president of LYNX Technologies (www.lynxtech.com), a tariff consultancy. Networkers need to look carefully and compare local pricing before negotiating. Often substantial reductions, at least as much as 69 percent, can be found.

MONTHLY LOCAL E1 PRICES WITHIN 75 TO 80 MILES*

Country	Tariffs	Market High	Market Low
United Kingdom	\$2,915	\$2,378	\$1,000
France	\$2,998	\$2,545	\$1,058
Netherlands	\$2,502	\$2,007	\$768
Germany	\$1,246	\$1,064	\$644

*The tariffs are based on the published tariffs or rates of the primary national carrier. The market rate ranges are based on rates taken from actual proposals and sales in those markets. More aggressive rates might be possible.

Source Lynx Technologies (Fairfield, NJ, www.lynxtech.com)

Europe Warms to Hotspots

Though Wireless LANs (WLANs) may be the United States's hottest remote access technology, some countries still give them the cold shoulder. The United Kingdom even makes it illegal to operate commercial services over the unlicensed frequencies used by WLANs, supposedly to protect private users of the technology. A December 2001 report to the British government recommended that this restriction be scrapped, but one company has decided not to wait. Regardless of what the law says, it plans to install Wi-Fi (IEEE 802.11b) access points at more than 4,000 hotels, railway stations, and pubs around the United Kingdom.

Surprisingly, the renegade isn't some scrappy start-up that wants to undercut the large carriers. It's venerable monopolist British Telecom (www.bt.com), which last year was forced to sell its cell phone division, mm02, in an attempt to repay debts incurred buying third-generation (3G) spectrum licenses. The expensive licenses went with mm02, leaving BT with no wireless assets, but it sees Wi-Fi as a cheap way to get back into the market. The company also hopes to offer managed WLANs

within offices, enabling further nodes to be added to its network at no cost.

While the United Kingdom hasn't yet approved wireless LAN services, it's taken another step towards improving WLANs themselves. Along with the Netherlands, it announced in April 2002 that it would allow the sale and (non-commercial) use of IEEE 802.11a equipment, which is currently banned in other European countries. 802.11a-based networks are about five times as fast as those based on regular Wi-Fi, and a larger allocation of spectrum means that more networks can share the same airwaves. However, this last benefit doesn't yet apply in the United Kingdom or the Netherlands, because much of the 5GHz bandwidth that 802.11a requires is still reserved for Europe's own HiperLan2 system. Vendors and the IEEE believe that 802.11h, a new revision of 802.11a so similar to the current version that it can be applied to existing equipment through a software upgrade, will secure approval in the entire band throughout Europe by the end of 2002.

—Andy Dornan, San Francisco

COUNTRY PROFILE



PRICING INFORMATION Telefonica

- Exchange rate: USD = 181.654 ESP
- Cost of 10 minute call to U.S. during peak hours: 331.00 ESP (\$1.80)
- Cost of a national call during peak hours: 21.40 ESP (\$0.12)
- Monthly rental of a 256Kbit/sec half circuit to the U.S.: 1,220,000 ESP (\$6,716.06)
- Monthly rental of a 2048Kbit/sec half circuit to the U.S.: 3,500,000 ESP (\$19,267.40)

Source: PBI Media (www.tarifica.com)

OVERALL DEREGULATION LEVEL: ● / ●

- Monopolistic; ● Some competition; ● Healthy competition

DEREGULATION STATUS

International leased lines	●
Domestic long distance leased lines	●
Access lines	●
International VSATs	●
Internet	●
International telephony	●
Domestic telephony	●
Wireless	● / ●

INTERNET/VOIP STATUS

Local loop	●
Long distance/National	●
International	●

DEREGULATION DETAILS

December 1998 Spain completes the liberalization of its telecommunications industry.

April 2001 Spain's government extends the deadline to roll out third-generation (3G) mobile phone networks from August 2001 to June 2002.

December 2001 The European Court of Justice upholds Spain's legislation requiring incumbent operator Telefonica to significantly reduce its interconnection and access fees to meet the European averages.

January 2002 Spain's Telefonica opens 62 of its exchanges in accordance with European Union standards to open up the local loop.

March 2002 Spain's telecommunications regulator gives the OK for Mobile Virtual Network Operators (MVNOs) to resell mobile services through third-party networks.

Regulator Telecommunications Market Commission (CMT)

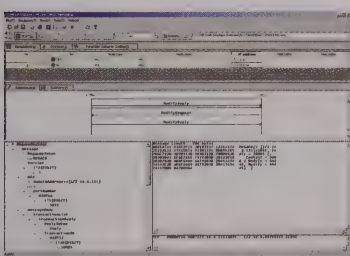
INCUMBENT CARRIER

Name	Services	Geographic coverage	Web
Telefonica	telephone, mobile, Internet, data	international, domestic, local	www.telefonica.es

**Superb operability
puts the world at your fingertips.**

Two powerful solutions from Artiza Promise optimal system performance.

Artiza Networks offers two advanced, yet highly affordable software applications to enhance the performance of any communications network. A proven success in their home market, they are now available worldwide via the Windows NT/2000/XP platform.



Artiza VoIP Simulator

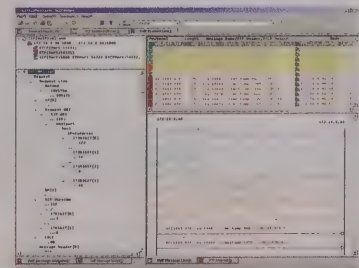
Enables setting of contents of signal message protocols, and the production, editing and running of sequence scenarios — simulating IP phone, VoIP gateway, gatekeeper, media gateway, media gateway controller, and others.

Real time messaging, simple user interface, audio assistance, many other functions.

VoIP Test Solutions

Collates IP packets upstream from the network to analyze and display VoIP protocol. Highly cost effective application features unique automatic message session detection, a wide selection of filtering functions, QoS evaluation support, etc. without requiring specialized hardware.

Artiza VoIP Analyzer



▶▶▶ Please visit our site, and download 14-day trial versions of our programs. ◀◀◀

Artiza Networks, Inc. <http://www.artizanet.com>

OpenReach's Frame Relay Plus

product spotlight by Doug Allen

IP VPNs continue to undergo serious market turmoil. Especially since the 2001 downturn, customers have been faced with uncertainties in terms of definitions, best practices, and ability to deliver on the technology. Serious doubts remain as to the reliability of IP, its Return on Investment (ROI), and the amount of “bang for the buck” companies receive. And while some providers have gained a few hundred customer wins or so, most end users haven’t taken the bait. Instead, they’ve stayed with their old, slow (usually 56kbits/sec), and more expensive frame relay. Many of these same network managers want to move to IP. It’s just a question of the migration path.

A slow, controlled pilgrimage to IP is the selling point of a number of IP VPN start-ups that use client software to set up and terminate full-function VPNs. The software is run on a server at each node of the network and controlled by a centralized NOC. This keeps deployment costs low, while providing end users with full onsite management capabilities. Because there’s no hardware or real CPE to speak of, one vendor refers to the resulting flexibility as “fluid networks.”

That vendor, OpenReach (www.openreach.com), is one leader in this space. Before you say “Who?,” this company has already amassed over 150 business customers. Their latest offering is Frame Relay Plus, a suite of three services—FrameFlow, FrameAid, and FrameGuard—that use IP VPNs to back up and extend the functionality of typical frame relay dedicated lines.

FRAMEFLOW

Addressing the need for greater bandwidth in the face of bandwidth-hungry applications such as file sharing, voice, or video over IP, FrameFlow allows the customer to offload high-bandwidth

traffic to an OpenReach VPN running over a separate T1 or DSL line, so that delay- or security-sensitive flows remain congestion-free on the frame relay pipe. The vendor claims a tenfold spike in frame relay performance in this scenario. Again, since most customers have a T1 already, the deployment cost is simply the desired number of servers and the monthly management costs for OpenReach’s NOC support.

FRAMEAID

FrameAid is a backup service designed to kick in when a primary line goes down. Typically, ISDN or some other low-cost connection is used, but as OpenReach points out, ISDN links are fair game to frequent events such as new area code or password assignments, or even a pulled wire. Proactively testing such a circuit isn’t possible with ISDN, so the only way to know if the line will fail is after the fact. FrameAid uses the same IP VPN approach as Frame Relay Plus to provide a low-cost secure backup to the frame relay line. FrameAid is always on, and is actively monitored, measured, and recorded so that it’s available when needed most.

FRAMEGUARD

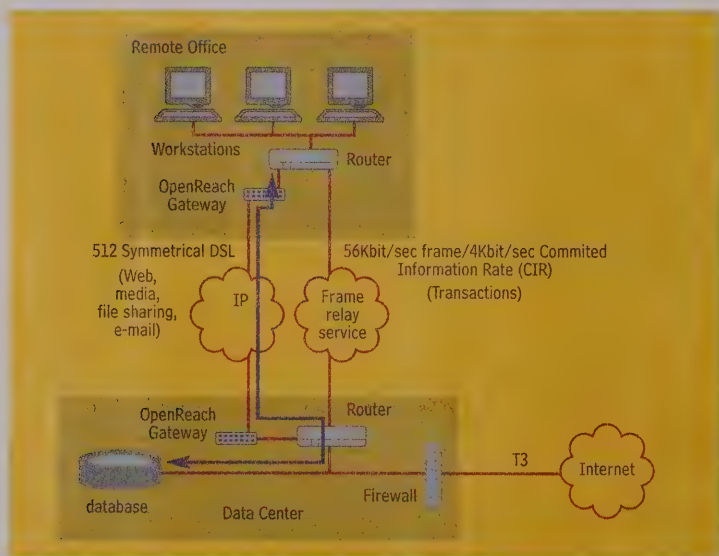
FrameGuard answers the problem of internal security attacks, where as much as 71 percent of cyber crimes are committed, whether through LAN snooping or hacks on individual PCs. Picking up where firewalls, private lines, and vanilla VPNs leave off, FrameGuard protects the “last yard” by securing the frame relay network and LAN with a built-in firewall, authentication of all outside users with digital certificates, and encryption of all traffic passing between the networks.

HIGH MARKS

“What appeals to me is that they’ve implemented a managed service version of an approach I’ve been advocating to our clients for a long time: VPNs to complement—not necessarily replace—traditional services like frame relay,” says Jim Slaby, senior industry analyst with Giga Information Group (www.gigaweb.com). “This is a great way to gain confidence in, and overcome the security objections to, VPN capabilities without betting the farm on the technology. And it matches horses for courses—for example, using cheaper, lower-grade bandwidth in places where the sacrifice in quality is worth it, which it clearly is in restoral and bandwidth-on-demand scenarios.”

Though not exactly a name brand, OpenReach does get strong marks from analysts and end users. One customer, Illinois Tool Works, a manufacturing company with hundreds of global locations, claims that it’s saved 30 percent on its communications costs while increasing performance by 300 percent. Obviously, results can vary, but when used tactically, software VPNs can be a low-risk way to go.

The Frame Relay Plus suite is currently available. Pricing varies by implementation. *



Horses for Courses. FrameFlow backs up the preferred frame relay line with a low-cost IP connection for less sensitive applications.

3G Wireless Works!

Faster deployment

Your choice of wireless carrier matters! CDMA carriers are the first to market with fully standardized, commercial 3G networks and devices—long before other wireless carriers. By choosing a CDMA carrier, you can leverage the real and practical advantages of 3G CDMA *today*, and avoid the pitfalls of a costly and complex wireless network and device migration path.

Faster network throughput

Today's 3G CDMA networks provide peak rates up to 144 kbps. But more importantly, they provide real throughputs of up to 60-90 kbps, enabling many applications that were never before practical over a wireless wide area network (WAN).

More device choices

With our industry-leading chipset and software solutions, QUALCOMM is enabling the rapid development of 3G devices by dozens of leading manufacturers worldwide. This includes PCMCIA cards with WAN access at up to 60-90 kbps for enterprise data applications such as e-mail, customer relationship management and sales force automation. Phones and PDAs with low-latency browsing, color displays, and increased capabilities for position location and enhanced wireless multimedia are also commercially available. (See www.3Gtoday.com for more details.)

Faster development

QUALCOMM has created an open applications platform called the Binary Runtime Environment for Wireless™ (BREW™) that supports native C/C++ and Java™ applications, enabling developers to extend enterprise applications quickly and easily. BREW also lets you download and update applications directly to the user's device for better software management and control.

Faster decisions

Our mobility experts at Wireless Knowledge deliver strategic mobility solutions that leverage existing investments while harnessing the technical and competitive advantages provided by today's 3G wireless technologies. By extending critical corporate applications to mobile devices, business professionals are empowered to make informed, financially justified decisions to drive their business.

Faster ROI

From improved productivity and responsiveness to better logistics and customer relationship management, the benefits of corporate data mobility are more compelling now than ever. Visit www.qualcomm.com/enterprise to learn more.



As president of QUALCOMM's Wireless & Internet Group, Dr. Paul Jacobs has a unique perspective on third-generation (3G) networks, devices and applications. How will 3G drive new advances in enterprise mobility?



Lesson 167: Security and 802.11 Wireless Networks

by Steve Steinke

Wireless LANs (WLANs) conforming to the IEEE's 802.11b specification have become popular, and there's every reason to think that 802.11a and 802.11g networks will also be widely deployed in the next few years. One attraction of these wireless networks is how easy they are to implement. Unfortunately, 802.11b networks suffer from various security shortcomings. Coping with these security problems is complex and potentially costly—possibly even negating the value of such networks.

Traditional LANs shared a single medium—a copper cable and passive hubs or concentrators. These hub ports and cable taps were almost always located within a facility with some physical security that made it nontrivial for an attacker to tap into. Many modern LANs associate a single switched port to each user, limiting the span of even an authenticated internal user, much less an outside attacker. By contrast, WLANs share an ill-defined medium in free space, which almost certainly includes locations outside the physical control of WLAN administrators, such as the company parking lot, other floors of the facility, or nearby high-rise buildings. For this reason, a wireless network is fundamentally less secure than a wired one.

Acknowledging the inherent security deficiencies of WLANs, the 802.11 committee adopted an encryption protocol called Wired Equivalent Privacy (WEP). Note the rather mealy-mouthed terminology: WEP isn't positioned to provide real privacy—just privacy comparable to otherwise unprotected wired networks. Furthermore, WEP isn't positioned to provide authentication, access control, or data integrity. However, the authentication and data-integrity capabilities provided by 802.11 networks are built on a WEP foundation, so if WEP is broken, so are these mechanisms. It turns out that authentication, data integrity, and access control on 802.11 networks can be broken without breaking WEP, but WEP's failure as an encryption protocol is nevertheless a serious problem.

What's at stake if WEP encryption can be defeated? An eavesdropper can, among other things, watch and intercept traffic flows, including e-mail, browsing, file transfers, and remote terminal sessions.

An eavesdropper can also map and capture all conversations on the network, including management and configuration processes, as well as end-user data; or capture IDs and passwords that users employ to log in to other networks and resources.

WEP DEFICIENCIES

How serious are WEP's deficiencies? Before answering that question, I'll first have to discuss how WEP operates. WEP uses a stream cipher named RC4, which means that it uses a shared secret key to generate an arbitrarily long sequence of bytes from a pseudorandom number generator. This stream is XORed with the plaintext to produce the encrypted ciphertext. (RC4 encryption works successfully with Secure Sockets Layer (SSL), the encryption protocol that lets you breathe easier when you use credit cards to make purchases on the Web.)

Early 802.11b networks used 40-bit keys because of the federal government's restrictions on encryption in those days, but most current components use 104-bit keys. Hackers can crack a 40-bit key with a brute-force attack in just hours with modern PCs, but for now, a brute-force attack on a 104-bit key would take longer than the current age of the universe, so there's little to worry about on that front.

It's easy to break RC4 encryption if a second instance of encryption with a single key—a keystream reuse—can be isolated. The WEP designers were aware of this problem, and they built into WEP a so-called Initialization Vector (IV), a 24-bit value that changes with each packet and is appended to the unchanging shared secret key to minimize the likelihood of “key collision.”

The IV is carried in the clear in each packet—otherwise the receiver couldn't set up the RC4 engine for decryption. Because 2^{24} is 16,777,216, it initially appears that an eavesdropper would have to capture many millions of packets to identify keystream reuse instances, but thanks to the “birthday paradox,” a key collision is likely to occur after only 5,000 or so packets. (The birthday paradox uses elementary

probability techniques to demonstrate that the odds are greater than even that, out of a group of 23 randomly chosen people, at least two of them will have the same birthday.)

If this problem weren't serious enough, Fluhrer, Mantin, and Shamir, in “Weaknesses in the Key Scheduling Algorithm of RC4” (see Resources, page 32), identified a further problem with RC4. This paper demonstrates that a fraction of the keys in RC4 are weak, revealing more of the structure of early bytes in the output than they ought to. By exploiting the statistical properties of this weakness, an attacker can crack any message in hours, independent

of other attacks. AirSnort (<http://airsnort.shmoo.com/>), one of the best-known WEP cracking tools, employs this attack.

Even assuming a less than fully loaded network, an attacker can create a full keystream dictionary in just a few days. Various vendor-specific implementation choices can reduce this crack time substantially. The 802.11 standard doesn't specify a key distribution method, so vendor algorithms generating shared secret keys from passwords might be subject to simple dictionary attacks that greatly reduce the problem of guessing the key. The general reliance on out-of-band—usually manual—key distribution ensures that keys won't be changed often. Attackers capable of sending data into the network can speed up the key-cracking process in various ways. (See “Intercepting Mobile Communications: The Insecurity of 802.11,” at www.isaac.cs.berkeley.edu/isaac/mobicom.pdf for more details.)

AUTHENTICATION ISSUES

Authentication failures result in unknown users on the network. An attacker who intends to crack WEP or misuse network resources must first authenticate successfully. (A large fraction of 802.11 networks are configured with the authentication system turned off, so a person who wants to attack one of these systems wouldn't even have to take the simple steps listed here.)





YOU'RE PROTECTED AGAINST HACKERS, VIRUSES AND WORMS.
BUT WHAT ABOUT ROSE IN BENEFITS?

eTrust™ Security Solutions

Complete protection for your entire enterprise.

When it comes to protecting your business, you need security that can protect your enterprise from potential threats, no matter where they may come from. That's exactly what eTrust does. Our family of products allows you to not only safeguard your entire enterprise, but also view and manage that security either centrally or from multiple delegated locations. So you can continue to grow and maximize new opportunities while minimizing your risk. And that's security you can feel secure about.



Computer Associates™

Resources

The Unofficial 802.11 Security Web Page, www.drizzle.com/~aboba/IEEE, has a comprehensive list of relevant materials.

"Intercepting Mobile Communications: The Insecurity of 802.11," by Nikita Borisov, Ian Goldberg, and David Wagner, can be found at www.isaac.cs.berkeley.edu/isaac/mobicom.pdf. This paper is one of the most clear and understandable descriptions of cryptographic subjects to be found anywhere. It explains WEP thoroughly and precisely and presents the problems associated with keystream reuse.

"Weaknesses in the Key Scheduling Algorithm of RC4," by Scott Fluhrer, Itsik Mantin, and Adi Shamir, can be found at www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf. The details provided in this paper are probably beyond the ability of security civilians, but these findings provide the basis for AirSnort, a widely available cracking tool. You can find out more about AirSnort and download the software at <http://airsnort.shmoo.com/>.

With a laptop outfitted with NetStumbler (www.netstumbler.com/), you can find unauthorized wireless networks, assess the reachability of authorized networks, or go war driving and find all the wireless access points in the neighborhood.

The protocol analyzers from Network Associates (www.nai.com), WildPackets (www.wildpackets.com), and Network Instruments (www.networkinstruments.com), among others, can decode wireless traffic when outfitted with supported wireless interface cards.

The 802.11 specification supports a two-step form of authentication. Potentially participating stations must respond correctly to a cryptographic challenge (the authentication step) and then associate with an access point by submitting the access point's Service Set Identifier (SSID.) The association step adds little security to the system—some vendors provide clients with a list of SSIDs to choose from. But all vendors broadcast the SSID values in the clear, so a protocol analyzer with a wireless card can find these values in seconds.

The authentication step relies on RC4 encryption, as WEP does. The problem isn't the insecurity of WEP as such, or of RC4 in itself. Again, it's an issue of implementation. An access point issues a cryptographic challenge by encrypting a

random string with the shared secret key using RC4. The initiator must decrypt the challenge and send the plaintext back to the access point, which compares the decrypted plaintext with the original random string. If they match, the initiator is authenticated.

By capturing only two frames—the challenge frame and a successful response frame—an attacker can easily derive a keystream that will successfully decrypt future challenges. An integrity check is built into WEP systems, presumably to prevent this replay attack. But the integrity check is based on the Cyclic Redundancy Check (CRC) mechanism that many data-link protocols use, and CRC doesn't depend on a cryptographic key, so it's easy to get around this obstacle.

In addition, attackers can use a well-understood method to make arbitrary changes to a message, so the checksum of the changed message is the same as that of the original. This data-integrity failure not only implies that an attacker can modify any content—for example, the position of a decimal point in a financial document—but it also lets attackers use the checksum to assess the correctness of their decryption attempts.

Properly authenticated and associated clients are often given full access to the wireless network. Even without cracking WEP encryption, attackers can access wired networks connected to the wireless one, and perform illegal, embarrassing, or otherwise undesirable acts that reflect badly on the network administration. Attackers can also spread viruses, Trojan Horse programs, and perform local or remote Denial of Service (DoS) attacks.

The 802.11 and WEP mechanisms say little about enhanced access control. Some access-point vendors build in a MAC address table that can serve as an access-control list, accepting traffic only from clients whose MAC address appears on the list. The problem is that MAC addresses are necessarily transmitted in the clear, so a wireless protocol analyzer can pick them up immediately. In general, you can configure wireless NICs with different MAC addresses, so a spoofing attack on this form of access control is trivial.

PROTECTIVE RESPONSES

It should be clear that the 802.11 families of wireless products share serious deficiencies in privacy, confidentiality, data integrity, and provisions for safety from various other attacks. That isn't to say that WEP is useless. A home network that isn't

connected to an enterprise network, isn't part of a commercial operation, and has no confidential, illegal, or embarrassing online content will provide little incentive for an attacker to defeat WEP authentication and encryption. Every other 802.11 network should be accessible only via VPN login or equivalent mechanisms.

Network managers should periodically audit their facilities for rogue 802.11 networks. Wireless traffic should be outside the enterprise firewall or within the Demilitarized Zone (DMZ). User-initiated wireless networks probably won't be outside the secure perimeter and offer a juicy target for attackers, whatever their motives. In fact, user-initiated networks are likely to be implemented without authentication and WEP, which is as big a security hole as can be imagined.

The principal deficiencies of 802.11 security are the result of security implementation by software and hardware engineers who lack sufficient understanding of real-world security. The security experts who criticized WEP implementation from the beginning weren't simply tooting their own horns. Some of the choices seem elementary, such as the use of CRC for integrity assurance.

Similarly, security textbooks emphasize that RC4 keys ought never to be repeated, not just limited to once every 16 million packets. No doubt there were performance, power consumption, and cost constraints that entered into the poor decisions. Every packet of an 802.11 wireless network requires a lot of processing work, and radios are often finicky performers. Wireless LAN implementations prior to 802.11b had lousy performance and no security, so even WEP was a step in the right direction.

The 802.11 committees are aware of these shortcomings. The 802.1X committee has defined a standard for authentication and key management for Ethernet and other 802-numbered data-link technologies that should eventually be integrated with 802.11 systems. Proposals to strengthen or replace WEP are also in discussion. All the problems identified so far can be addressed, but delays of months or years are almost certain where standards organizations are concerned. In the meantime, the need to add security features beyond those built into the 802.11 protocols will undermine the attractive simplicity of wireless networks. *

Steve Steinke, editor-in-chief, can be reached at ssteinke@cmp.com.



FOR A HEALTHY BUSINESS, TAKE ONE REGULARLY.

ITU TELECOM events are telecom-related exhibitions and forums that are the most important supplement to your normal business diet.

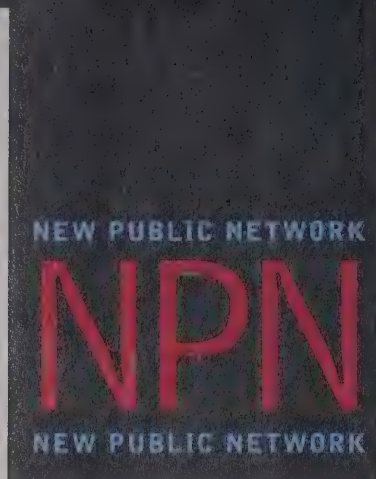
They bring together the biggest exhibitors, the most incisive forum participants and the most influential visitors with a keen interest in everything to do with making a healthy living in info-communications.

So make sure you've got the dates of the ITU TELECOM events in your diary.

www.itu.int/itutelecom

telecominf@itu.int
Tel.: +41 22 730 6161 Fax: +41 22 730 6444

ORGANIZED BY THE
INTERNATIONAL TELECOMMUNICATION UNION (ITU)



What does the future hold for networking?
We asked leading thinkers in the areas of
carrier services, security, and Web services.

by David Greenfield

Crystal Ball Gazers

Ever wish you could gaze into the future? Imagine the strategic advantage, not to mention the financial advantage, of spotting the switching revolution or the Internet boom years before they occurred.

While crystal ball sales might be nonexistent, *Network Magazine* stirred up its own version of wizardry. We cornered some of the best minds in the industry and found out where they think the hot spots will be over the next three years. Some of these networking geniuses are well established names, others are folks immersed in the technology. All had fascinating insights about the future of carrier services, application integration, and security.

If their predictions are any indication, companies haven't even begun to scratch IP's and the Internet's potential. Remote offices will increasingly connect through VPNs across an IP network, and Voice over IP (VoIP) will be hotter than ever with integrated voice-data applications. Companies will also use IP to enhance application integration within companies and potentially between companies. Of course, all of this presupposes that critical holes in network security can be addressed (see figure on page 37).

A revolution will take place in integrating secured mobility and process automation. "Three years from now, we'll know how the mobile revolution went—did 3G [third-generation] make it? Has XML [Extensible Markup Language] been useful? And were we able to deploy IPv6 without disrupting everything on the Internet?" says

Vinton G. Cerf, senior vice president of Internet architecture and technology for WorldCom (www.worldcom.com). "I'm not going to try to predict the answers, but I'm hoping for a positive outcome. It won't happen without a lot of work on the part of a great many people."

BANDWIDTH INFRASTRUCTURE SERVICES

Despite the Internet crash, the services space remains a vast forest of service providers: application service providers, ISPs, upstart competitors, and just about every type of hybrid possible. Over the next three years, these enterprise services will likely become more complex and sophisticated, due to IP's enhanced role.

At the infrastructure layer, local loop limitations will continue to confound the industry. "Overcoming the limitations on bandwidth in the last mile will continue to be a challenge. The economics of this problem, to say nothing of its thorny policy brambles, will make this a hard problem for some time," says Cerf.

For corporate networks this means that carriers will still labor to deliver *dependable* broadband IP connectivity backed by SLAs, says Pradeep Sindhu, founder and Chief Technical Officer (CTO) of Juniper Networks (www.juniper.com).

Meanwhile in the public network's core, lowering costs and enhancing adaptability is the name of the game. "Increased capacity in the core optical network and, in particular, the ability to run regenerator-free networks will have a

material impact on scalability and cost of operation," Cerf says.

Of course, part of this low-level infrastructure doesn't require fibers or wires at all. The emergence of wireless networks based around the 802.11 specification, along with protocols such as Bluetooth, will play a critical role. "My belief is that this area will evolve over the next couple of years, beyond the level of simply transport, to address issues such as content and delivery, reliability, and security, which is really bad," says Hossein Eslambolchi, AT&T chief technology officer and president of AT&T Labs.

An integrated voice-data IP network will emerge across this physical infrastructure. Part of this IP push will be the continued growth of VPNs, both in the WAN and for enterprise Wireless LANs (WLANs). The other part of the driver for VPNs is the use of Peer-to-Peer (P2P) technology or grid computing, where computers are combined to form a distributed supercomputer. "If internal [enterprise] use of P2P technology takes off, which it could, it will become a huge factor in this arena. A close relative of P2P and grid computing will probably take off only in the scientific space during this period," says Eslambolchi.

The upshot is that VPNs will become the dominant means for interconnecting corporate networks. "Increasingly, we'll see VPNs overtake traditional approaches such as private lines," says Eslambolchi, who says the push for VPNs is a big deal for AT&T.

Visionaries:

The Crystal Ball



The push towards IP will play a major role in the application space, as well. Certainly this means increased development of low-level applications services such as remote storage and computer services, network-based firewalls, network-based encryption services, and streaming services including voice and video. "The driver behind these services is basic economics: It is simply cheaper to offer this set of services when the equipment is on the provider's side of the network where the capital and operational costs can be amortized over a large number of users," says Sidhu.

Above these "facility" services common applications will metamorphose into an IP centric world. "The upper layers, including the control of sessions [that is, signaling, convergence of voice and data into higher level services], are now starting to emerge. They appear to be heading in the direction of SIP [Session Initiation Protocol]," says Eslambolchi. The result is integrated voice-data applications, such as advanced 800 services with Instant Messaging (IM).

Part of the push towards IP telephony also involves the Electronic Numbering (ENUM) initiative. In March 2002, *Network Magazine* exposed the political wrangling behind this benign protocol that provides a standard translation between a DNS name and a phone number (see "The Clique Cracker," March 2002, page 52). According to Cerf, ENUM will create a thunderous revolution among telephony providers, making it possible to bring out services that interconnect or interlink many different modes of communication, including fax, phone, e-mail, voice mail, video, and so on.

Ultimately, mobility and IP will merge. "Internet-enabling of all kinds of mobile devices, coupled with IPv6 deployment and 3G or 802.11a or b, could create a diverse and interesting platform for new products and services," says Cerf. "Adding speech recognition into the mix makes it even more interesting, as new services become conveniently accessible."

"I get very excited about having billions of Internet-enabled devices around, because one can then imagine assembling subsets of these, on the fly, to provide a product or a service," he says. "For example,

I'm driving down the street and through my mobile phone I ask a speech-understanding computer where the nearest ATM is. A map pops up on the independently IP-addressed navigational display, while a voice says over the car speakers, 'it's two blocks up and to the right.' Or, I ask for the location of the nearest Thai restaurant. Again a map pops up and the speaker says, 'do you want to see or hear the menu? Make a reservation? Place an order for pickup?' Perhaps in a few years I won't need the ATM, because I'll be able to download money into my personal digital assistant, but I'll still be very interested in the pad Thai and lemon grass shrimp soup."

Internet-enabling of all kinds of mobile devices could create diverse and interesting platform for products and services.

BUSINESS PROCESS AUTOMATION

Both Eslambolchi and Cerf see the real pot of gold in automating supply chains. Supply-chain vulnerabilities

remain a critical problem for even the biggest companies. According to a report published by Forrester Research (www.forrester.com), General Motors, for example, was forced to reduce quarterly earnings in 1996 by \$900 million because an 18-day labor strike at a brake supplier factory idled workers at 26 assembly plants. Boeing lost a deal worth \$2.6 billion in 1997 because two key suppliers failed to deliver critical parts on time.

Web services frameworks, such as Microsoft's .Net or Sun Microsystems's J2EE Enterprise Edition (J2EE), promise a way out by enabling processes on different computers to pass data using HTTP, the same protocol used for passing Web traffic.

"This is a huge area that is taking off in a number of ways," says Eslambolchi. "They include Web services, which will take advantage of the powerful, but loosely coupled nature of the Web, to provide applications such as Customer Resource Management (CRM), Enterprise Resource Planning (ERP), supply-chain management, and direct customer ordering or trouble ticketing. This area will change the face of business, not by a single technology, but by a combination [of technologies], including Artificial Intelligence (AI), software dependability, and information mining."

Cerf agrees and again sees mobility as playing a key role. "I expect to see considerably more inter-enterprise communication

to occur with the use of XML-encoded business transactions," he says. "Many of these transactions will be authorized and authenticated using Internet-enabled mobile devices. Some will use 3G or 802.11a or b transmission systems to achieve mobile data access."

These services will also be more regionally targeted. Cerf sees increased value in geographically indexed databases, as Global Positioning System (GPS) capabilities become more common. "In some cases, such as automobiles, the local auto network will supply GPS information to any device online in the car. That could mean literally being plugged into a wired LAN, but might also be a wireless local network," he says.

But not everyone thinks Web services will be used to link companies together any time soon. Mike Rosen, a chief enterprise architect at IONA Technologies, a provider of Web services, thinks the technology will be crucial for integrating applications within the enterprise over the next three years. Inter-corporate integration faces a variety of challenges.

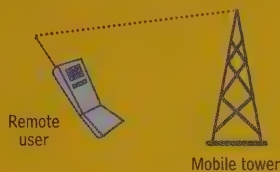
"Most activity around Web services today is internal application-integration projects," says Rosen. "Web services are already opening up new opportunities to simplify integration greatly. At the same time, ERP and application vendors, such as SAP and Oracle, are busy providing native Web services interfaces to their applications. It turns out that application integration is the 'killer app' for Web services, which will increasingly be used as a technology for tying together applications and business processes replacing existing, proprietary technology."

Inter-corporate engineering will face several problems in the future, says Rosen. Until these problems are resolved, which will take more than three years, small companies won't be able to simply visit a Web site in order to locate a business partner or establish a secured supply-chain connection across the Internet in minutes.

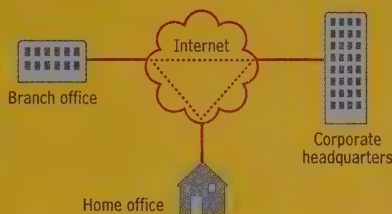
Internet security is a huge and familiar issue (see "The Next Wave in Distributed Processing, April 2002, page 38), but network managers will need to be sure Web services suppliers address other, less well-publicized problems as well.

Take the problem of extended transactions, for instance. Today, there's no generalized protocol for rolling back transactions across multiple databases. Suppose a PC manufacturer, such as Dell, orders and then cancels a shipment of networking cards from 3Com. 3Com can

Hot Spots in the Network of Tomorrow



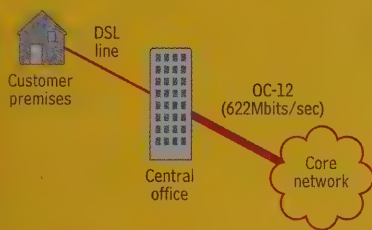
Mobile, Mobile, Mobile. Roaming users will be able to initiate transactions and run client-server applications from the field.



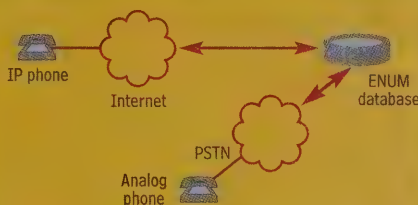
VPNs. Forget private line and frame. The network of tomorrow will increasingly run over VPNs.



Supply Chain Automation. Look for Web Services to integrate applications and ultimately automate supply chains.



Local Loops. Opening up the local loop bottleneck will continue to be a problem.



Voice Over IP. Drop those old phone lines. With the advent on ENUM and SIP, VoIP will finally fulfill its promise of lowering cost and enabling new applications.



Network Security Challenges. As business partners, mobile users, wireless networks and home users get connected, network security becomes a paramount concern.

Networking Hot Spots. Here are six ways your network is sure to change over the next three years.

either build the cards anyway or find a way to roll back the database to the initial state before Dell's order. This may entail rescheduling workers, notifying and canceling supply shipments, and freeing up assembly lines. A lot of today's business models don't account for these steps.

Reliable message delivery is another major problem. Today, if something goes wrong with a Web request, users just refresh their browsers, but if that request was "cancel my order for 50,000 network cards," you need a mechanism that guarantees message delivery. Application-integration environments, such as IBM's MQ-Series, understand these issues well. The HyperText Transfer Protocol-Reliability (HTTP-R), committee and the Microsoft Global XML Architecture (GXA), some of the groups spearheading Web services development, are now grappling with these issues.

Moving further down the supply chain, shared context becomes a hot issue. Sensitive customer information must be passed along, so each company in the supply chain can read that information and change it appropriately. A travel site, for example, might want to add a new service allowing customers to arrange for flower pickup at a specified destination. To add a

florist easily, especially in the case of small florists, the travel site needs to be able to pass information about the customer's identity, his or her credit card number, and arrival time. This implies a range of questions that need to be answered: What information will suppliers in the chain be able to see and alter? What are the security policies governing those changes? How are those changes made? And, finally, how will these problems be regulated?

After answering these questions, you can address problems such as licensing. How will developers pay for a Web service? What's required? Will they pay a one-off fee? Is this something they'll pay for on an ongoing basis? If so, how will licensing be monitored and work over a message complying with the Simple Object Access Protocol (SOAP)? (This protocol is a method of encapsulating messages in XML and serves as the basis for Web services.)

NETWORK SECURITY

Security headaches are even worse than supply-chain problems. The key challenge to security will be the corporate infrastructure's expansion. Today, intranets are expanding beyond traditional corporate walls out into the Internet through

mobile, wireless, and VPN connectivity. Corporate security systems will need to account for increasing external, as well as internal, threats.

Traditional defense systems, such as firewalls and Intrusion Detection Systems (IDS), are becoming obsolete, while the perimeter becomes more and more porous," says Philippe Courtot, chairman and CEO of Qualys (www.qualys.com), a producer of security auditing services. He points to easy use of HTTP and Secure Shell (SSH) protocols to tunnel content through firewalls carrying Web services traffic. "VoIP will only exacerbate the problem and be an important driving force for the convergence of voice security, QoS, and data networks through TCP/IP," Courtot says.

And as mobility continues to spread in the workforce, networkers will need to be even more careful. "Now you have PDAs and BlackBerry used by traders for communicating back to the corporate premises in an unsecured fashion," says Jerry Ungerman, president of Check Point Software Technologies (www.checkpoint.com).

Perhaps, though, the biggest threats are internal problems. The advancement of productivity software architectures also

Resources

To learn more about Extensible Markup Language (XML) and Simple Object Access Protocol (SOAP), visit www.w3schools.com.

You can find network security information at many sites. One of the more entertaining and informative ones is www.securitygeeks.shmoo.com. It provides lots of free-form discussion about various security topics.

Want to learn more about Electronic Numbering (ENUM)? Go to www.enum.info, www.enum.org, and www.ngi.org/enum.

You can learn more about the Microsoft's Global XML Architecture (GXA) at <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dngxa/html/gloxmlws500.asp>.

increases external security threats. As software suppliers look to lock companies into suites by integrating more functions into their products, the networking environment gradually becomes homogenized, says Martin Roesch, founder and CEO of Sourcefire (www.sourcefire.com), a provider of IDSs. Roesch is the author and lead developer of the Snort Intrusion Detection System, the first open-source IDS on the market.

Centralizing software functionality could lead to productivity improvements and simplified network management. However, this process also makes the network uniquely vulnerable. The more homogenous the network, the more likely a single attack will decimate the entire network infrastructure, notes Roesch. "The analog in nature is particularly clear: Undifferentiated ecosystems are extremely fragile whenever an outside contagion is introduced. The same concept applies to the homogenous enterprise environment," he says.

The result of this homogenization is an increased number of mobile code attacks. The attacks use code that's portable across applications, such as Microsoft's macro language. "Mobile code attacks led to repeated e-mail viruses that terrorized corporate IT managers since the I.Love.You virus made its debut," says Roesch. Vendors have tried to address the problem by integrating virus detection, secure execution environments, mail filters, and other technologies with marginal success, he contends. "This problem isn't going away. It's getting worse as mistakes are repeated and amplified in OS design, letting things

such as e-mail scripting languages make direct calls at the OS level," he says.

Internal employees will also need to be monitored more closely. "Enterprises deployed massive network infrastructure over the past 10 years, and up until recently never really thought much about the concept of trying to monitor the activity on those networks for both 'health' and security," says Roesch. "Network-management systems are available, but the information they relay is only as accurate as the agents are capable of communicating back to the management interface. While this is a great way to manage the network generally, monitoring what's really happening on a network should be the domain of the intrusion-detection and network traffic-analysis applications," he says.

Even then, gathering data isn't enough. "These applications are in fairly wide deployment, but the essential piece of the puzzle is managing all the data they produce in an intelligent and useful way and being able to provide feedback to the network-sensing, access-control, or intrusion-prevention mechanisms that are available as part of this network-monitoring infrastructure," Roesch says.

While many corporations are taking measures to address the problems of internal monitoring, they're ignoring the mobile-code problem. "The threats represented by mobile code and homogeneity aren't widely recognized at this time and require a lot more education of both the corporate and government community, although mobile code is recognized as a danger within the security community at this time," says Roesch.

Are there reasons to be concerned about things like cyber terrorism, a phenomena Roesch readily dismisses? "It's hype," he says. "The big problem right now is with computers connected to physical infrastructure, power companies, and SCADA [Security, Control, and Data Acquisition] systems used in surveillance cameras. These are all vulnerable to real-world attacks through their computer networks, although the necessary knowledge is rather esoteric, and terrorists, such as suicide bombers, seem to prefer real-world acts where they kill many people at close range."

The government's involvement in addressing these issues should be nominal. "Overall, legislation in itself is the wrong paradigm," says Dr. Arvind Krishna, vice president of IBM's Tivoli security products. "Market incentives to increase computer security will prove to be superior. Thus,

lower business risks, lowered costs, improved profits, and superior user volume scaling will drive improved security, not government measures," he says.

Roesch is even more critical of government involvement. "The legislative arm of the government is catering to corporate interests with the laws it's proposing these days," he says. "Look no further than the Security Systems Standards and Certification Act [SSSCA] legislation from Senator Fritz Hollings from South Carolina. This legislation is nothing more than a big wet kiss to media and software companies that wish to legislate their business models back to legitimacy."

While Roesch might dismiss the government legislation in the area of security, he's much more excited about the side of government that defends itself from constant Internet attacks. "These parts of the government can be very helpful to the industry, sharing their experiences and lessons learned with corporate organizations that are still on the steep information-security learning curve.

"The government knows pretty well what problems it faces, from what I've been able to see, and it's willing to take the measures required to get secure," Roesch continues. "This stands in stark contrast to corporate America, which talks about the urgent need for security solutions on the one hand and continuously under-budgets for the real needs that it pays lip service to on the other."

FINAL SPIN

Over the next three years, fundamental changes will affect the services delivered and the providers selling them. "I would say that we will see a revolution on the systems side of what we do [that is, operations and high-level services]," says Eslambolchi. "This can change the very nature of how we think about CIO functions, and about the delivery of systems services. The revolution is driven by the advances in hardware [chips and disks], software [Web services, scale, and reliability], and security [VPNs]. It includes concepts such as virtual integration. But the bottom line is that there are order of magnitude changes in the size and sophistication of what can now be done, and the winners are getting on board now." *

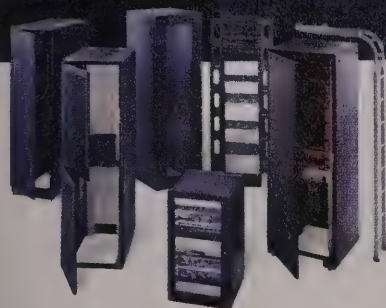
David Greenfield, international technology editor, is the author of The Essential Guide to Optical Networking, published by Prentice Hall. He can be reached at dgreenfi@cmp.com.

Hoffman

A Pentak Company

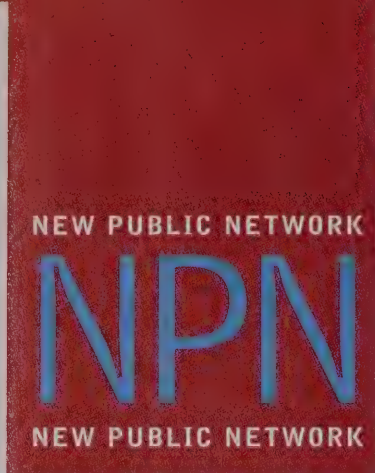


Are racks and cabinets the last thing on your mind?



You don't think about racks, cabinets and enclosures every day. But we do. We're obsessed with building the best. Millions of them every year. Built-to-order. With more accessories and options. Delivered fully assembled. Fast. A complete selection available locally, nationwide. Hoffman. 763-422-2211. Keep us in the back of your mind.

www.ehoffman.com



Apps that combine voice and data are starting to emerge. But do end users really want these features?

by Doug Allen

Convergence in the Enterprise: Does Anyone Care?

When you hear the phrase “next-generation voice services,” what comes to mind? Do you think of Voice over IP (VoIP)? Or do you envision a world of vague, but interesting, value-added applications resulting from the marriage of voice and data?

If you’re like me, you probably view transport and QoS as a necessary evil, and applications as the sexy part. Though lower costs are part of VoIP’s appeal, it’s the services that will push end users into the world of converged applications.

There’s been little development of such services that don’t replicate old Time Division Multiplexing (TDM) Class 5 switch functions in the data world. In fact, when softswitches came around three years ago, separating the transport layer from the call control and signaling layers that make up the PSTN, the industry press seized on the possibilities of converged applications that end users and business groups could buy to meet their specific needs. Innovation, thine hour is at hand!

But, it didn’t work out that way. This article explores the reason for this by looking at these new applications, their usefulness, and whether or not customers really want or need them.

NEW DIRECTIONS IN VOIP

First, the softswitch market has yet to gather momentum. Though vendors such as Sonus (www.sonus.com), Telica (www.telica.com), Nortel Networks, and even

some RBOCs and Interexchange Carriers (IXCs) have announced significant wins, this doesn’t mean services are available yet. Although softswitches have proven successful at Internet offload and Class 4 switch functionality, they haven’t established themselves as Class 5 replacements. Many vendors and some analysts feel this leap is inevitable—the main argument is when the RBOCs and carriers will move to converged services in a big way. But it probably won’t happen in 2002 or 2003.

In the meantime, many start-ups focused on convergent applications are bringing IP PBX and IP Centrex features, such as unified messaging, to businesses. These vendors either sell directly or partner with a softswitch vendor like Sonus to reach providers such as Touch America (www.tamerica.com), Masergy Communications (www.masergy.com), or voice Application Service Provider (ASP) TalkingNets (www.talkingnets.com).

For instance, Sonus has many partners that only do enhanced converged applications, such as BayPackets (www.baypackets.com) for Internet call waiting, voice and unified messaging, and voice VPN; NetCentrex (www.netcentrex.net) for call center and Automatic Call Distribution (ACD) features; and Voyant Technologies (www.voyanttech.com) and Pactolus Communication Software (www.pactolus.com) for conferencing services.

Sonus and other softswitch vendors or provider customers have also partnered

with Broadsoft (www.broadsoft.com), which along with Sylanro (www.sylanro.com), is leading the IP Centrex charge. Other key players in this space include LongBoard (www.longboard.com) and VocalData (www.vocaldata.com). These companies also compete with pure IP PBX vendors, such as the more established Shoreline Communications (www.shoretel.com), and staples like Lucent Technologies and Nortel.

“Up and coming” best describes these companies. Broadsoft reports that the IP Centrex players have 12 provider wins, with tens of thousands of lines installed, and expects substantial growth in 2001. Sylanro claims 10,000 end users from its service provider customers alone, mostly in the United States, but also internationally, and especially in vertical markets such as real estate, banking, travel, and construction.

“The size of the implementations ranges from very small offices to distributed enterprises of 400-plus people,” says Laura Thompson, vice president of corporate marketing at Sylanro. “Service-oriented industries have been among the strongest adopters, due to features that facilitate their handling of customer calls—such as advanced find me/follow me and rules-based call forwarding.” Shoreline’s sweet spot is the multisite enterprise with 100 to 3,000 employees. It has racked up over 340 customers, many deploying VoIP gear at new locations (see figure, page 42).

THE VALUE PROPOSITION

Today, customers use convergent applications for services that mimic Class 5 features, with a Web GUI simplifying management via a visual interface with point-and-click, drag-and-drop simplicity. However, convergent apps' real value lies not in parity with the PSTN, but in enabling new applications that unlock competitive advantage and differentiation. The result is slow but steady growth in IP Centrex solutions for small and medium-sized businesses (SMBs).

These convergent applications must also be easy to use, require minimal disruption (that is, work with existing telephones instead of upgrading to IP phones), and provide a smooth and controlled migration path to an all-IP solution at low per-user monthly rates.

Because of all the fear, uncertainty, and doubt surrounding new features, a major selling point is the ability to customize all voIP services through the GUI. Capabilities must include centralized moves, adds, and changes abilities for either a network administrator or an end user. One such change might grant an employee long distance calling privileges to only specific numbers at certain times of the day, week, or month, and then revoke the privilege, based on business rules. The GUI should display relevant billing data to that employee or manager,

as well as missed/inbound/outbound call logs and online directories.

Also important is the ability to assign features to specific commands. Instead of remembering complicated strings of star codes to execute a special feature on a digital phone, end users can create shortcuts linking a simplified icon command to a given function, such as moving extensions, setting up new users, or implementing a speed dial or follow-me feature.

Vendors such as Sonus use Session Initiation Protocol (SIP) to communicate between next-generation voice platforms customized through scripts and service-creation environments. You can modify Sylantro's platform via the Web, Microsoft Outlook, a Wireless Application Protocol (WAP)-enabled cell phone, or the LCD display on a desk phone. Shoreline goes a step further. Using Telephony API (TAPI)-based apps, you can distribute features throughout all sites in an enterprise voice network. "End users can take control of any standard phone, IP or analog, at any company office with a PIN number," says Barry Castle, vice president of marketing at Shoreline. "Then all communications—voice, e-mail, voice mail, and so on—shift to that desktop," he says.

If these apps work, the result should be something like a voIP intranet, providing all linked company employees with a uniform, feature-rich set of services—for free.

Dave Passmore, research director of the Burton Group (www.tbg.com), refers to it as a single virtual PBX. This feature is especially useful for particular vertical markets, such as medical and finance, which can leverage voIP apps for call forwarding services, among others.

A KID IN A CANDY SHOP

Let's daydream and turn an uncritical eye to some of these converged apps. First, there's IP PBX, a Customer Premises Equipment (CPE), IP data-enabled version of a traditional PBX and its functionality, including proprietary feature sets, customizable star or number codes for features, and so on. You can easily assign these features to a desk phone with a few clicks on the GUI.

IP Centrex is more popular, with more new lines added. It supports traditional (TDM) Centrex but adds network-based apps such as PBX functionality, auto-attendant, voice and unified messaging, conferencing, call center and ACD functions, Instant Messaging (IM), and "hot desking." This last feature transfers a user's feature set from his or her usual office phone to any other phone.

These are the table stakes for the new players, but additional functionality is also available or in development, and of course, you can customize all these features to end-user requirements. Presence-management features are also starting to come on strong, where users can see if the person they want to call is available, on the phone, in a meeting, and so on. Some platforms will even tell you when a person you're trying to reach gets off the phone, then automatically dial the number.

Another popular feature these converged apps offer is unified messaging. This includes visual voice mail, or e-mail access over the user's phone through Interactive Voice Recognition (IVR), possibly with a customized notification system that pings you when you have a new message. The "find-me/follow-me" feature rings users at the desired location (desk phone, home phone, cell phone), based on the identity of the caller, the time of day, or both.

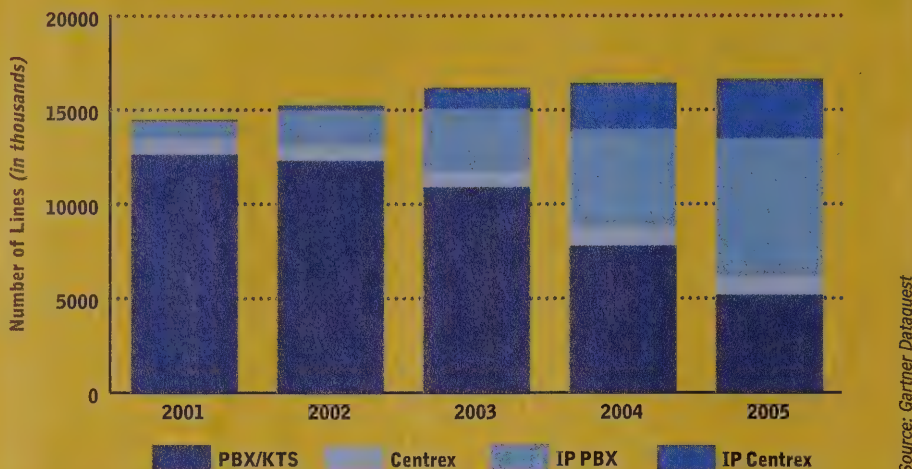
Other features are VIP calling, also called "selective forwarding," which can forward a particular phone call to a specified employee's desk, if the first user doesn't pick up; and click-to-call, which allows users to click on or select a voice mail icon to dial that caller's number automatically. Most next-generation vendors will include online directories and incoming call logs to



Illustration: Steven Weissman

IP Centrex, IP PBX, and Legacy Projections

New Enterprise Line Shipments (not installed base)



The Future of Convergence. Customers won't likely swap out their installed base of PBX/KTSs (Key Telephone Systems), but future IP line shipments are set to grow quickly over the next three years.

facilitate this feature. These logs can be accessed remotely.

With these capabilities, some vendors are marketing service bundles aimed at specific, though still broad, business markets. For instance, Sylanro sells c-Business, which provides core business-communications features, such as hosted PBX (network-based, not at the customer premises) and IP Centrex functionality, with directory and browser-based functions and mobile phone-type features, such as call logs, click-to-call, and single-number support. Sylanro's ComCierge service packages a variety of find me/follow me features and personal call commands that use caller ID. On the call center side, ComMerchant provides automatic call-distributor handling.

Several vendors are also trying to head off provider integration issues by focusing on Operational Support System (OSS) issues. LongBoard is the best example of this, focusing on next-generation apps that link Microsoft Outlook with other voice features, while including hooks that talk to telcos' back office systems for billing, provisioning, and so on. LongBoard's platform is essentially a service-creation tool environment enabling developers to create customized applications, a much-hyped but little-realized advantage of an open system.

LongBoard is banking on mixing control call management with Microsoft Outlook and presence features to support new

hybrid apps composed of Web pages, VoIP, and IM and presence services. An example of this is listing all co-users currently on the network at any particular time, or setting up a call to a specified group at a specific time, when they're all available.

Nortel envisions collaborative messaging that allows co-workers to share files, Web pages, and interactive whiteboard sessions in real time. To simulate the experience of "being there," users would need to know who's on the call, who's speaking, whether someone's raising his or her hand to speak, and be able to have side conversations via text chats, and so on. This won't likely happen for quite a while.

The logical outgrowth of many of these features is "session level control, such that within a given session you can move among various media," says Christine Hartman, research director of VoIP markets at Probe Research (www.proberesearch.com). "So, perhaps you start by sending an instant message asking if I have time to talk. We talk over the phone for a few minutes before I send a picture of a concept I'm working on. We then agree to meet, but before we do we escalate the session to video, so we know what the other person looks like."

WHAT DO YOU REALLY WANT?

This all sounds great, but does anybody want this stuff? It turns out few people do. Early adopters aside, there's been little mass-market penetration. Why?

Lack of imagination is one problem. "When buyers were presented the proposition that voice services could be 'programmed' to suit their needs [in a focus group study], and given some examples, they were immediately capable of defining 'new' services," says Tom Nolle, president of CIMI Corp. (www.cimicorp.com). "Most of these (about 85 percent) turned out to be nothing more than customizations of existing services, such as call forwarding with automatic time-of-day cancellation."

Simply customizing existing services leaves VoIP app potential untapped, and makes it hard to justify the business case. Most businesses look at voice mail, auto-attendant, and maybe voice e-mail with language and notification options as table stakes, and not much more, according to Stevan Vigneaux, president and CEO of Iperia (www.iperia.com), an app server vendor that focuses on subscriber features like the ones previously listed. Beyond these basics, enhanced VoIP apps are a tough sell for CFOs.

"Buyers [from the aforementioned focus group] could not, without prompting, come up with any suggestions for new apps," says Nolle. "Our conclusion: These apps could be developed with marketing effort, but probably can't pull through spontaneous changes. Users don't plan for things that aren't offered in the carrier service set, so they're bad at conceptualizing what they might want."

Part of the problem, says Nolle, is that buyers can't assess the Return on Investment (ROI) of a given app, contrary to several vendors' claims. "Our surveys, going back to the early 1980s, have consistently shown that buyers aren't a reliable guide for what they might buy if it were available, only on what they will buy of the collection of currently available services."

"One of the problems we face today is that often the people developing and funding the next generation are not representative of the general population," says Probe's Hartman. "Many technical people thrive on resolving complex problems, so the services they tend to create are complex, when what the larger market wants is simplicity."

Often, VoIP buyers will invest in new gear for the cost savings. They're certainly aware of a migration path to converged apps, but are likely to begin using them slowly. The features alone don't necessarily motivate the sale. In contrast, most prospective buyers won't buy simply to lower costs—they want advanced

**Open.
Install.
Profit.**



Sprint North Supply and ADTRAN deliver network solutions packaged to fit your needs. Take Sprint North Supply's leading-edge logistics network, e-business capabilities and significant deployment experience. Add ADTRAN's NetVanta 2000 series for a complete high-speed VPN and firewall solution and secure communications over Internet and IP networks. Include a reassuring five-year warranty and you've got a solution ready to serve your network needs today and tomorrow.

Think Sprint North Supply and ADTRAN.

[www.sprintnorthsupply.com 800.755.1950]



Sprint North Supply



Resources

For more on softswitch architecture, deployment, standards, interoperability testing, and industry news, check out the International Softswitch Consortium at www.softswitch.org.

For more on IP Centrex features, applications, benefits, and vendor/provider information, go to www.ip-centrex.org.

The best Web sites for information on converged apps are the vendors themselves, and a few providers. We recommend TalkingNets (www.talkingnets.com), Broadsoft Communications (www.broadsoft.com), and Sylanro (www.sylanro.com) for white papers, case studies, and testimonials.

Nortel Networks has an extensive tech paper on these apps called "Are You Ready for IP telephony—10 Things to Look for in our Data Network." Go to www.nortelnetworks.com/products/01/succession.

functionality to justify the purchase, too. This leads to a catch-22: Which comes first, the features or the cost savings? The jury's still out, if only because so many of the benefits of enhanced features remain unproven. Given this, why should a network manager move to VoIP, when TDM is so reliable?

Aside from the drawback of deploying IP phones, "the business has little motivation as long as the current method [the PSTN] works," says Hartman. "The RBOCs don't appreciate how much their system pisses off the general public unless a competitor offers something better." In other words, wait for the other guy to do it first. Given that RBOCs have traditionally separate bureaucracies for voice and data services, who don't always play nicely together, this could be some wait.

The crux of the issue, though, is do these apps solve real business problems? "I think it's specific to the business," says Deb Mielke, principal of Treillage Network Strategies (www.treillagenet.com). "Unified messaging is cool, but does everyone really need it? I think it's good for consultants and folks on the road, but does the guy who never leaves the office require that kind of functionality?"

Maybe these value-added apps don't have enough perceived value. "The current emphasis in VoIP is big on parity with TDM features," says Hartman. "But rather

than solving [replicating] a feature the same way with VoIP, we need to look at what need drove the feature and ask whether there's a better way to solve the same problem. Take call waiting. My money is on the person who figures out a better way to fulfill that service, so that it doesn't interrupt the current conversation. Caller ID helps, but it still breaks my thought patterns."

Most observers agree buyer education is a big obstacle. How can providers build demand for services when end users often don't know they exist? "Microsoft Outlook has a feature that lets people with modems use them to dial voice calls," says Nolle. "Not only does hardly anyone use that feature, hardly anyone knows it exists." IP Centrex vendors echo this refrain regarding PSTN star code features.

But providers have big problems when it comes to educating the public, especially in the SMB sector. "Who [at the provider level] is going to educate this space?" says Mielke. "The 20-year-old salespeople that carriers dedicate to this space? In this market salespeople have to do volume. Are you really going to spend your time educating? I think SMBs are waiting for someone to tell them what they need and how it will make their business more profitable."

LOOKING FOR INNOVATION

So we're back to our catch-22, where both providers and SMBs are looking to each other for answers. Where will innovation come from? Smart bets are on the large enterprise. Traditionally, SMBs don't have the in-house expertise or enough provider support to come up with new, proprietary apps. In contrast, large businesses have a "let's do it ourselves" attitude and have more IT staff for support chores. So, while SMBs will probably go to a VAR that pitches them an IP PBX, the big boys are likely to create business-specific apps for themselves that increase productivity and profit margins.

"Connectivity within closed user groups of people with a strong need to communicate offers a test bed for controlled experimentation," says Hartman, who cites voice mail as an example. Initially, people used voice mail at work, and it took a while to catch on in the home. But then it took off as the advantages became obvious. Some of these new proprietary developments will migrate to mainstream systems (if not patented), even if they aren't designed for the mass market.

Of course, human factors always come into play. Just as many people don't like talking to a machine to leave a message, user habits will constrain adaptation of new apps. Do enough potential users want to access their voice mails visually, such as with e-mail? No one knows.

WHAT TO LOOK FOR

If you're brave and feel that the features are compelling enough, you might want to find a provider for outsourced, preferably managed, VoIP services. A number of basic provider constraints mitigate against quick deployment of these services, especially from RBOCs. Numerous testing, OSS, interoperability, end-user device, and business models (ROI) need to be worked out. But from an IT staff perspective, it makes sense to outsource if you can't manage the system in-house, or if it's not a core task, as long as you save money, streamline your business processes, or even present a more high-end business image.

When shopping for a provider, make sure you're satisfied the company will be alive in six months. Aside from financial viability, the provider should have geographic network reach corresponding to your own locations, a simple, brief training curve with adequate long-term support, and a smooth, minimally disruptive installation process. Competence in voice and data and simplified management processes are a must.

Dave Passmore, a Talking Nets and Broadsoft customer with an Ethernet phone, notes a couple of pain points to watch out for. Voice quality can be constrained by too much compression (say, at 8kbps/sec), so make sure you can get higher-quality codecs, up to 64kbps/sec. Backup power isn't guaranteed, so if the power goes out, you'll need redundancy, possibly by using cell phones. And beware of delays with the RBOC, which may take a few days to update its number portability database to accommodate your new phone number.

You'll also need to dig deep to ascertain if the necessary support staff is in place. How large is the staff, and what's their average current call hold time? Be sure to ask for a dedicated support representative who wants to help you maximize the services you've already purchased, not upsell you on something you might not need. ☼

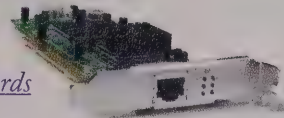
Doug Allen, senior editor, can be reached at dallen2@cmp.com.

*"Mission Critical" shouldn't
refer to your tech budget.*

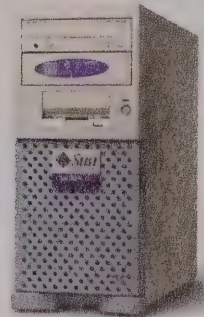
Routers



PCI Cards



Workstations



Telephones



Monitors



NICs



*For great finds on more networking gear than
you can possibly imagine, check out eBay.com.
AOL Keyword: eBay*

eBay[®]
happy hunting[™]

Storage Networking: Fibre Channel, IP, and Beyond

How will Fibre Channel, IP, and emerging interconnect technologies shape the new networked storage landscape?

by Elizabeth Clark

For years, storage has been viewed as a necessary evil, but it's becoming increasingly essential to the health and well-being of today's enterprise network. Over the past year, developments in storage networking have mushroomed, and nonstop efforts to standardize emerging approaches have confused many organizations seeking alternatives to their current storage strategies.

To help eliminate some of this confusion, this article examines existing and emerging approaches to storage networking, focusing primarily on Fibre Channel, IP-based storage alternatives, and a new interconnect technology that could significantly impact storage networking in the future.

CHANGING CHANNELS?

Fibre Channel is a standardized technology that has overcome many of the interoperability issues that plagued its youth. Fibre Channel is a block-level (as opposed to a file-level) transport technology with some relatively advanced QoS features, including guaranteed packet delivery. It's typically faster to access block-based data than the file-based data that Network Attached Storage (NAS) systems transmit. You run Fibre Channel on a separate network, which can help address congestion and security issues.

Fibre Channel preserves the basic command codes of SCSI, the block-based protocol that transmits data to and from Storage Area Network (SAN) storage arrays. Therefore, hardware vendors can migrate from SCSI to Fibre Channel without a major overhaul. The recent introduction of 2Gbit/sec switches has also revved up Fibre Channel.

According to Eric Sheppard, senior research analyst at IDC (www.idc.com),

Fibre Channel will continue to be the interconnect of choice for SANs through 2005 to 2006. (For information on anticipated Fibre Channel-related product revenues, see the figure on page 47 and the table on page 48.)

On the down side, Fibre Channel is limited to 10 kilometers, and it's still pricey. Although nobody's going to rip out an existing SAN, not everyone is bullish on Fibre Channel's long-term future. "Fibre Channel is a major pain to administer," says Lauri Vickers, an analyst with In Stat MDR (www.instat.com). "Maybe you're already stuck with some legacy Fibre Channel stuff, but do you really want to keep adding to it?"

STOCKING UP ON IP

Given IP's growing popularity, it was only a matter of time before the industry began eyeing IP for storage traffic. Enter IP storage, the transfer of block-level data over IP-based networks. IP is a well understood and relatively inexpensive technology, with many supporting products and services. IP is compatible with Fibre Channel and Gigabit Ethernet, with the latter providing an opportunity to overcome Fibre Channel's distance limitations. The upcoming 10Gbit/sec Ethernet will be another boost for IP-based storage, which can then be used more efficiently for applications such as remote mirroring, replication, electronic vaulting, and for linking distant SAN "islands."

But IP storage takes some hits when compared to Fibre Channel's performance, reliability, and security. IP is still a best-effort service, and Ethernet's 1500-byte maximum frame size can render transmission of IP data less efficient than transmission of Fibre Channel packets. Depending on the implementation, IP storage can also require hefty hardware and software changes, but products in this area remain relatively sparse.

IP storage product vendors will also have to employ a standard method of encoding and decoding storage transmissions to avoid interoperability problems. To overcome Fibre Channel's limitations, and to help address some issues entailed

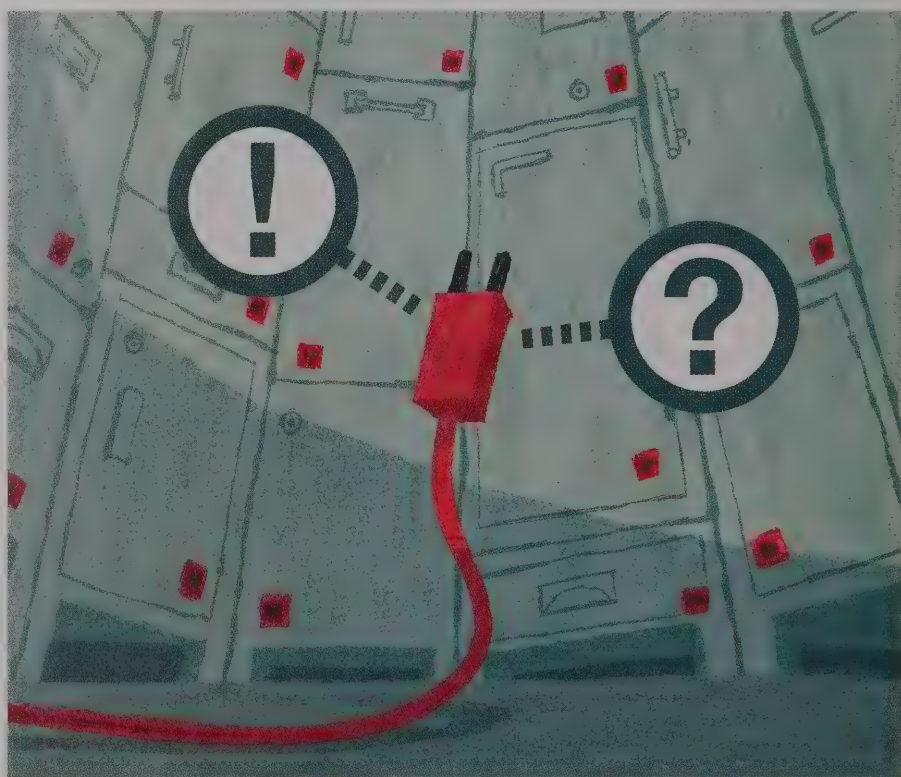


Illustration: Pep Montserrat

in IP-based storage, industry members have submitted many standards to the IETF.

SCSI GETS A TUNE-UP

One standard is Internet SCSI (iSCSI), which enables transmission of SCSI commands over TCP/IP. Cisco Systems and IBM originally submitted iSCSI to the IETF for consideration. The Storage Networking Industry Association (SNIA) is also backing iSCSI. Although proponents have touted impending ratification, the protocol wasn't standardized as of press time.

In iSCSI, the SCSI command set is mapped to IP for transmission of block-level data. Like Fibre Channel, iSCSI preserves the SCSI command set. But a native iSCSI network would cut Fibre Channel out of the picture, and could be run over a standard Ethernet connection. The ultimate vision for many proponents is end-to-end iSCSI SANs, which could be built using iSCSI-enabled devices such as tape libraries and disk arrays, along with iSCSI host adapters and IP switches.

While there's been speculation about the possibility of iSCSI replacing Fibre Channel technology for some applications, this probably won't occur soon. Because few devices with native iSCSI interfaces are now available, the two technologies will likely coexist.

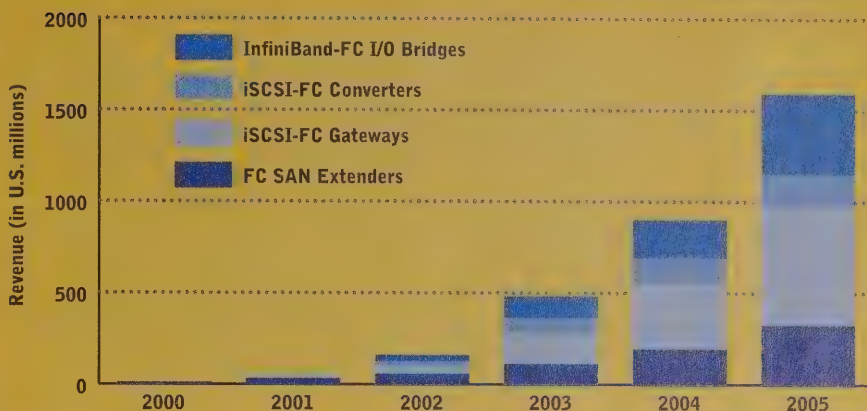
Arun Taneja, senior analyst with the Enterprise Storage Group (www.enterprise-storagegroup.com), says iSCSI will most likely debut in the networks of small and medium-sized businesses, primarily at the lower end of the market. According to IDC's Sheppard, volume end-user adoption of iSCSI SANs will begin in 2003. (For projections on iSCSI-related equipment revenues, see the figure on this page and the table on page 48.)

One of the earliest iSCSI-compatible devices was Cisco's 5420 Storage Router, introduced in 2001. The router links iSCSI devices to Fibre Channel systems. Other vendors, such as Nishan Systems (www.nishansystems.com), 3ware (www.3ware.com), SANcastle (www.sancastle.com), and FalconStor Software (www.falconstor.com) have rolled out iSCSI-compatible switches, servers, and software. Among the iSCSI-compatible equipment are modules that convert Fibre Channel ports to iSCSI-compatible IP ports.

As it turns out, iSCSI might end up giving NAS technology a run for its money. "iSCSI is really competing with NAS, not with Fibre Channel," says Randy Kerns, senior partner with The Evaluator Group (www.evaluatorgroup.com).

Storage Network Bridging Forecast

Source: Gartner Dataquest, November 2001



Crossing the Divide. Vendors will offer different methods for bridging technologies such as Fibre Channel, iSCSI, and InfiniBand. These include Fibre Channel extension products for connecting distant SANs, modules and gateways that link iSCSI- and Fibre Channel-based systems, and bridges that connect InfiniBand- and Fibre Channel-based systems.

Like NAS, iSCSI can handle file-level I/O, but it can also process block-level data. iSCSI is most likely to appear first in small workgroup and departmental settings—the turf NAS has historically grazed on. In contrast, iSCSI's speed increase could bring NAS closer to the performance levels of Fibre Channel SANs.

An early entrant in the iSCSI market was IBM, which last year announced its TotalStorage IP Storage 200i, an iSCSI-based NAS device. Other vendors, such as Network Appliance (www.netapp.com), Quantum/ATL (www.quantumatl.com), Hewlett-Packard, and ADIC (www.adic.com) say they'll be introducing iSCSI-compatible products.

One knock on iSCSI is that mapping SCSI commands to IP introduces hefty processing overhead, which could result in latency. Host Bus Adapters (HBAs), designed to offload this TCP/IP processing from server CPUs, have been in the works. Vendors such as Intel, Adaptec (www.adaptec.com), Agilent (www.agilent.com), Alacritech (www.alacritech.com), Emulex (www.emulex.com), and QLogic (www.qlogic.com) have HBAs in varying levels of testing and deployment, but these products will have to become more widely available before iSCSI takes off.

iSCSI will also require modification of existing applications. Software will need to perform tasks such as detecting dropped packets and performing integrity checks—tasks implemented in hardware on Fibre Channel. While implementing

some of the TCP/IP protocol stack in hardware will help alleviate this problem, it won't make it vanish overnight.

Storage management software vendors, such as FalconStor, Bakbone Software (www.bakbone.com), and DataCore (www.datacore.com), say that they'll support iSCSI. Strong proponents of IP technology, including IBM, Cisco, and Nishan, are most likely to stand firm behind iSCSI. EMC (www.emc.com), Brocade (www.brocade.com), and McData (www.mcdata.com) have also indicated they'll support iSCSI in future products. However, few iSCSI products are now available.

STRETCHING SANs

Another alternative storage networking technology is Fibre Channel over IP (FCIP). Initially proposed by a group of vendors including Lucent Technologies and Cisco, FCIP has been submitted to the IETF for ratification, but it hasn't yet achieved final approval. SNIA also supports the standard.

In FCIP, Fibre Channel frames are encapsulated and tunneled over IP to connect distant SANs linked via an IP backbone. FCIP creates point-to-point connections between the remote SANs, overcoming Fibre Channel's distance limitations.

FCIP satisfies SCSI's guaranteed delivery requirements, without the need for a cumbersome reengineering process. But FCIP's use of tunneling could be an obstacle, because processing encapsulated packets can negatively impact efficiency and

Storage Area Network Technologies

End-Use Revenue (in U.S. millions)	Actual	Forecast						CAGR
	2000	2001	2002	2003	2004	2005	2006	2001-06
Fibre Channel SAN	1,275.8	1,904.1	2,037.0	2,010.7	1,932.9	1,633.1	1,435.0	-5
Percent of market	100	100	98	88	71	51	36	
iSCSI SAN	0.0	0.0	28.1	137.7	392.0	752.5	1,259.7	159
Percent of market	0	0	1	6	14	23	31	
InfiniBand SAN	0.0	0.0	23.6	128.0	383.0	818.1	1,320.6	174
Percent of market	0	0	1	6	14	26	33	
Total	1,275.8	1,904.1	2,088.8	2,276.5	2,708.0	3,203.7	4,015.4	16
Percent change		49	10	9	19	18	25	

Source: In-Stat/MDR, February 2002

Segmenting SANs. According to In-Stat/MDR, iSCSI and InfiniBand SANs will experience significant growth rates by 2006. Although Fibre Channel SANs will still claim the largest share of the SAN market by then, this segment is not expected to experience a growth rate commensurate with the iSCSI and InfiniBand segments. However, it's important to note that there are very few iSCSI and InfiniBand products available at this time.

speed. In addition, FCIP can be more susceptible to link failures than some other SAN extension technologies.

FCIP has received mixed reviews. "I think that it's a temporary technology, until the iSCSI standards are done," says Enterprise Storage Group's Taneja. "FCIP will be less impactful over time because tunneling isn't very effective."

"In the enterprise data center, you're going to see a lot of SAN-to-SAN connectivity over FCIP," says The Evaluator Group's Kerns. The fact that Fibre Channel is well entrenched in the data center will foster the adoption of FCIP in this environment, he says.

Despite lacking a standard, vendors have started releasing products based on FCIP. The technology can be implemented in devices such as switches, routers, bridges, and gateways, as well as in IP routers with FCIP-compatible blades, or in Fibre Channel switches with FCIP-compatible ports.

CNT's (www.cnt.com) UltraNet Edge Storage Router supports FCIP and will include iSCSI support in the future, according to the company. Lucent's OptiStar EdgeSwitch storage router, SAN Valley's SL1000 IP-SAN Gateway, and SANCastle's GFS-8 Global Data Fabric Switch enable connection of distant Fibre Channel SANs over long-haul networks, including optical links.

Most vendors of FCIP-compatible systems say they'll ultimately incorporate

support for iSCSI and InfiniBand, an alternative interconnect technology, into their products. (I'll discuss InfiniBand later in the article.)

FCIP isn't the only game in town for long-haul transport scenarios. Companies such as CNT, Inrange Technologies (www.inrange.com), and Akara (www.akara.com) offer products that can transport storage data over WANs and MANs, via technologies such as ATM, SONET, Dense Wave Division Multiplexing (DWDM), and dark fiber. While these approaches can provide some performance and reliability gains, products in this arena are pricey. And typically, you'd have to use the same vendor's product at both ends of a connection.

Because FCIP is essentially a Fibre Channel perpetuation strategy, vendors such as Brocade, McData, and Gadzoox (www.gadzoox.com) are among its proponents. EMC also says it will support FCIP. But as with iSCSI, be aware that few FCIP products are available.

Because of its limitations, FCIP probably wouldn't experience a high adoption rate for use within SANs. Rather, organizations that have already invested in Fibre Channel, and are looking for ways to stitch together their remote Fibre Channel SANs, would be more likely to use this approach.

A PRESTANDARD COLLAGE

Internet Fibre Channel Protocol (iFCP) is an alternative to FCIP. Initially proposed

by Nishan Systems, iFCP is a TCP/IP-based gateway-to-gateway protocol where Fibre Channel is mapped to IP. Like the other Nishan-sponsored specifications discussed here, the IETF hadn't ratified iFCP at press time.

Essentially, iFCP supplants Fibre Channel switches and routers with IP-based systems, while retaining the ability to link Fibre Channel devices via IP. By providing fabric services, as well as connectivity, iFCP could be used between distant SANs and within Fibre Channel SANs. In linking distant SANs, each end device on the SANs requires gateway hardware. These gateways would be compatible with iFCP and iSCSI, and iFCP would require fewer changes to existing Fibre Channel devices and applications, according to proponents. And in iFCP networks, the impact of link failures is minimized by iFCP's routing characteristics.

Nishan's IPS 4000 switch supports iFCP, iSCSI, and Gigabit Ethernet. While some vendors support iFCP, it remains largely a Nishan-sponsored entity.

iFCP is an IP-based technology, so it's theoretically more of a threat to Fibre Channel than is FCIP. Fibre Channel vendors point toward its lack of industry support. "iFCP is really only implemented by one company, whereas FCIP is implemented by many companies," says Camden Ford, senior product marketing manager with Brocade. "From a business perspective, iFCP just has no traction in the market."

But Tom Clark, director of technical marketing with Nishan, says FCIP's tunneling requirements might hinder efforts to leverage existing IP investments. For example, says Clark, "Tunneling doesn't offer any way to integrate with iSCSI. iFCP was designed to link together Fibre Channel end devices, but also accommodate plugging in iSCSI over time."

Vendors of IP switches, routers, and other systems would be the most likely to support iFCP. But much more vendor support is needed for iFCP to prevail in the market. EMC is adhering to its traditional "wait-and-see" approach. In addition to iSCSI and FCIP, EMC has also announced its intention to support the iFCP protocol. "We're not betting the boat on any one of them," says Paul Ross, EMC's director of network storage marketing. "We're going to support all three [technologies] and be ready, depending on which one plays out where."

Nishan has submitted other proposals to the IETF. One of these is Metro Fibre

Channel protocol (mFCP), which is geared toward data centers and short-haul networks such as MANS.

Another proposal, Internet Storage Name Server (iSNS), is based on SNS, a device discovery protocol for SANS. iSNS combines characteristics of SNS and DNS, the principal device discovery mechanism for IP networks. While iSNS has the potential to enhance the performance and management of mixed Fibre Channel-IP networks, it needs to garner support from many more vendors to pick up steam.

Nishan has coined its amalgamation of iSCSI, iFCP, and iSNS "Storage over IP" (soIP). Note that soIP is now a proprietary term, as opposed to its broader, more generic application in the early days of IP-based storage networking.

INFINIBAND INSIDE

Another emerging technology that could impact storage networking is InfiniBand. This 2.5Gbit/sec interconnect technology, developed by Intel, was intended to replace the geriatric PCI bus. InfiniBand was originally designed to be implemented in silicon, but will likely become much more than an internal bus replacement.

The InfiniBand Trade Association developed the InfiniBand architecture. This association includes Intel, Compaq, Dell, IBM, Hewlett-Packard, Microsoft, and Sun Microsystems. Other vendors, such as Brocade, Cisco, EMC, Hitachi, Lucent, and Nortel, have become sponsoring members of the association.

The InfiniBand specification outlines a point-to-point switched fabric, designed to allow multiple I/O devices to send requests simultaneously to the system CPU without introducing a bottleneck. InfiniBand's provision for direct memory-to-memory communications, in addition to its low latency and TCP/IP processing offload capabilities, makes it a promising candidate for enhancing the performance of applications such as server clustering.

InfiniBand could also enable enhanced scalability at lower costs. Early implementations of InfiniBand will likely be interconnecting server clusters in large data-center environments. The technology could eventually enjoy widespread use as a storage and network device interconnect.

InfiniBand is unlikely to supplant Fibre Channel SANS. Instead, it will probably coexist with technologies such as Fibre Channel, SCSI, and IP. One way to accomplish this is through InfiniBand-enabled bridges, switches, and routers.

InfiniBand could also improve the speed and performance of NAS systems. In this scenario, Direct Access File System (DAFS) could be leveraged to reduce the latency levels of NAS devices. DAFS, spearheaded by Network Appliance, is a protocol designed for file sharing in data-center environments. Network Appliance says it will introduce InfiniBand-compatible systems in early 2003.

But InfiniBand has some drawbacks. It's much more complex than PCI. Changing the physical I/O infrastructure could be a major headache, and compatible hardware and software must be developed. InfiniBand also has distance limitations that could prevent widespread extension beyond the data center. In addition, the technology might find itself competing against 10Gbit/sec Ethernet in the data center. Finally, native InfiniBand, which would further enhance performance, isn't on the immediate horizon.

Taneja says that InfiniBand will expand outward in the future. "The more I look at InfiniBand, the more I think that over the next four years it has the potential to go all the way to storage [environments]," he says.

"InfiniBand is inevitable," says Kerns. "But we won't see [native] InfiniBand-attached storage for several years." For projections on InfiniBand-related equipment revenues, see the figure on page 47 and the table on page 48.

Most vendors of Fibre Channel (and FCIP-compatible) equipment have indicated they'll incorporate support for InfiniBand into their systems. Many vendors, mostly start-ups, have developed or are working on InfiniBand-enabled servers, bridges, switches, and routers.

Mellanox Technologies' (www.mellanox.com) Nitro is an InfiniBand-based blade server for data-center environments. Crossroad Systems' (www.crossroads.com) Crossroads 1000 router enables transmission of data between Fibre Channel, iSCSI, and InfiniBand networks. Paceline Systems (www.pacelinesystems.com) says it will soon launch an InfiniBand-based switch that provides connectivity for servers, storage, and network devices.

Other vendors of InfiniBand switches, routers, and bridges include InfiniCon Systems (www.infiniconsys.com), InfiniSwitch (www.infiniswitch.com), and Voltaire (www.voltaire.com). Vendors such as Intel, JMI (www.jmi.com), and QLogic are just beginning to deliver InfiniBand HBAs. And Lane 15 (www.lane15.com) and Vieo (www.vieo.com) have been

Resources

To find out more about IP-based storage technologies, including Network Attached Storage (NAS) and Direct Access File System (DAFS), go to the Storage Networking Industry Association's site at www.snia.org.

For more information on the InfiniBand specification, go to the InfiniBand Trade Association's site at www.infinibandta.org.

You can find background on the Internet SCSI (iSCSI) specification submitted to the IETF at <http://search.ietf.org/internet-drafts/draft-ietf-ips-iscsi-11.txt>.

IP SANS: A Guide to iSCSI, iFCP, and FCIP Protocols for Storage Area Networks, by Tom Clark (Addison-Wesley, 2001, ISBN 0-201-75277-8) provides a comprehensive overview of IP-based storage technologies.

developing InfiniBand management software. But real-world implementations remain scarce.

NOT SO FAST ...

So, what does all this mean for the network manager? It depends. If you're with a small to mid-sized organization that doesn't have a SAN, iSCSI might be a good fit. If you already have Fibre Channel SAN, and want to extend it over a long distance, you might consider FCIP. If your storage network consists of Fibre Channel and IP-based systems, you might consider iFCP. If you want to boost the performance of server clustering in the data center—or rev up your NAS systems—InfiniBand could be the best option.

Ultimately, the prevailing technologies will coexist. "The future [of storage] is going to be heterogeneous," says Nishan's Clark. "Vendors who hope to be successful have to realize that."

But these technologies won't be adopted overnight. Product availability and lack of standardization remain gating factors. And interoperability issues are bound to surface.

The adoption of these emerging storage networking technologies is a long-term proposition, and might not make sense for some organizations. To more effectively plan your long-term storage strategy, you need to closely monitor developments in this area. *

Elizabeth Clark, executive editor, can be reached at eclark@cmp.com.

Behavior-blocking technology gives administrators a leg up in the race against zero-day exploits.

by Andrew Conry-Murray

Behavior-Blocking Stops Unknown Malicious Code

Signature-based anti-virus (AV) software is running a losing race. Malicious code writers persistently outpace the efforts of AV researchers to identify and halt the latest threats. This isn't due to a lack of effort: vendors have cut response time from days to hours. This is an admirable feat, considering they must ensure that the update detects and removes the virus, and that it doesn't interfere with the normal operations of their customers' myriad computer systems.

The problem is the race itself. Malicious code writers have a head start—they launch malware against live targets before AV researchers can analyze and counteract that code. Even if traditional AV vendors can release updates fast enough to protect nine-tenths of their customers, that still leaves one-tenth to deal with the damage. What network manager wants to be a sacrificial lamb, thrown to the wolves to save the rest of the flock?

And the virus problem is getting worse. According to ICSA Labs' 2001 virus prevalence survey, the likelihood of a company experiencing a worm or virus increased 15 percent in 2001. Average server downtime due to viruses was 14 hours. The median time to recover from a virus disaster was four person-days. (The study categorizes a disaster as 25 or more PCs or servers infected simultaneously.)

Traditional AV products clearly can't keep pace with the current threats. Many organizations are now investigating other options to fill the gap between virus attack and signature update. One such option is behavior-blocking technology, which has been around for several years, but is now gaining considerable traction because it provides what signature-based AV solutions can't: real-time protection against unknown malicious code.

Behavior blockers watch ActiveX, Java applets, various scripting languages, and other mobile code that arrives on a host via e-mail, the Internet, or other network connections. Some blockers isolate this code in a "sandbox," restricting the code's access to various OS resources and applications. Other blockers insert themselves into the kernel of a host's OS to intercept system calls.

From either vantage point, behavior blockers monitor the code as it runs in real time. If the code attempts a function that violates a predefined policy, the behavior blocker will halt that function (see Figure 1). You can also program behavior blockers to quarantine or kill

code and send a variety of alerts. It's this comparison of real-time behavior against a predefined rule set that enables behavior blockers to thwart zero-day attacks.

This article explores behavior-blocking technology, its benefits and drawbacks, and looks at several players in the market. It also discusses the future of signature-based AV software and whether behavior-blocking technology will support—or displace—its counterpart.

BEHAVIORAL SPECIALISTS

Companies turn to behavior blocking for two main reasons, says Dave Kroll, vice president of marketing and security research at Finjan (www.finjan.com), which makes behavior-blocking software. The first reason is to close the window of vulnerability. This window is defined by the time between the release of a new virus or worm onto the Internet and the creation of an AV signature that can be distributed to end users.

"It's a major headache to roll out emergency anti-virus updates," says Kroll. Administrators must reach every PC in the organization, including headquarters, branch and remote offices, laptop-toting road warriors, and home workers. Even a handful of PCs missing the update can compromise an entire corporate network.

Proactive solutions give harried administrators time to update signatures, apply software patches, reconfigure firewall

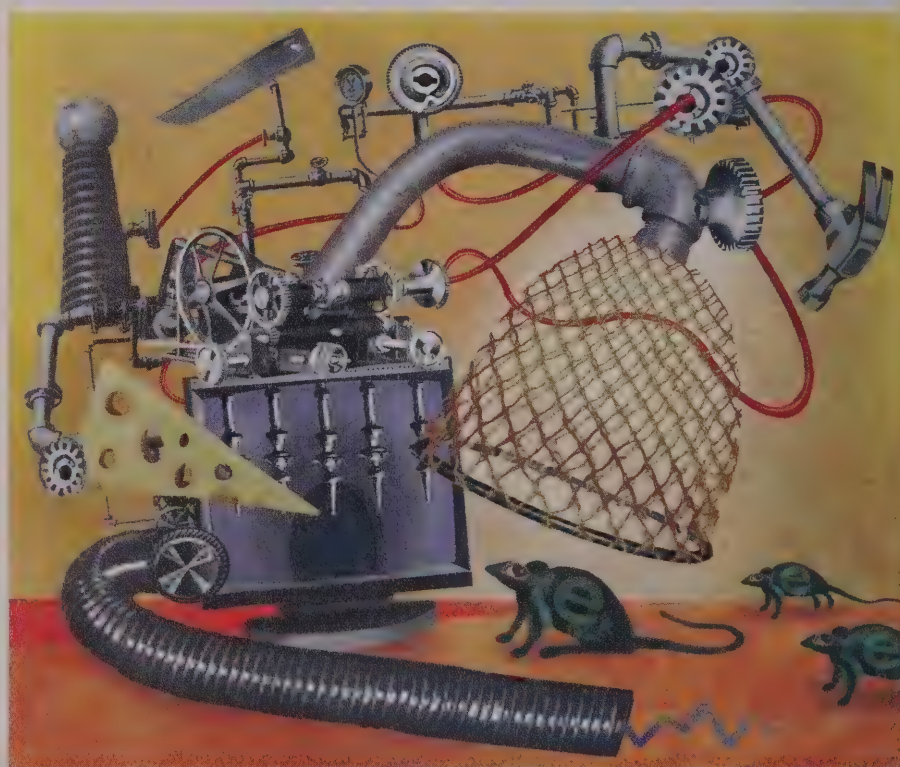


Illustration: Victoria Kann

rules, and take other steps to lock down the enterprise network. "If behavior blocking stops one or two viruses or worms a year, it's paid for itself," Kroll says.

The second reason companies use behavior-blocking software is that it's policy-based. Depending on the product, administrators can define very granular policies for specific departments, applications, and even end users. This granularity lets organizations distinguish between executable code that enables essential business functions and executable code that is either malicious or frivolous.

Ironically, policies are also often cited as a drawback to behavior blocking. Because the technology relies so heavily on policies, the burden is on the administrator to create a tight set of instructions for a host of applications, OS functions, and user groups. Poor policies will either halt benign processes or allow attacks to slip through.

This brings up a second flaw in behavior blocking: false positives. Like Intrusion Detection Systems (IDSs), behavior blockers are prone to trigger alarms for non-malicious events. False positives have the same effect as the boy who cried wolf. "If you get too many alerts, you're going to start mistrusting the system," says Vince Weafer, senior director of Symantec Security Response. Weafer says too many false alarms will encourage admins to ignore future alerts, or to turn the system off.

Despite these drawbacks, behavior-blocking technology has made headway in the security market. The next section examines several players and their offerings.

PRODUCT LINEUP

Finjan

Finjan leads the behavior-blocking market, according to analysts at IDC (www.idc.com). Finjan has three offerings in the behavior-blocking space: SurfinGate and SurfinGate for e-mail, which guard the gateway, and SurfinShield, which sits on desktop PCs.

At the gateway, SurfinGate inspects HTTP and FTP traffic for the presence of ActiveX, Java, Visual Basic Script (VBS), and JavaScript. It scans this code in real time for potentially malicious behavior, such as file-system operations and network operations. If such behavior is detected, SurfinGate checks it against an administrator-defined policy. If the action violates the policy, SurfinGate stops the code from entering the network, logs its action, and sends an alert to an administrator. Policies

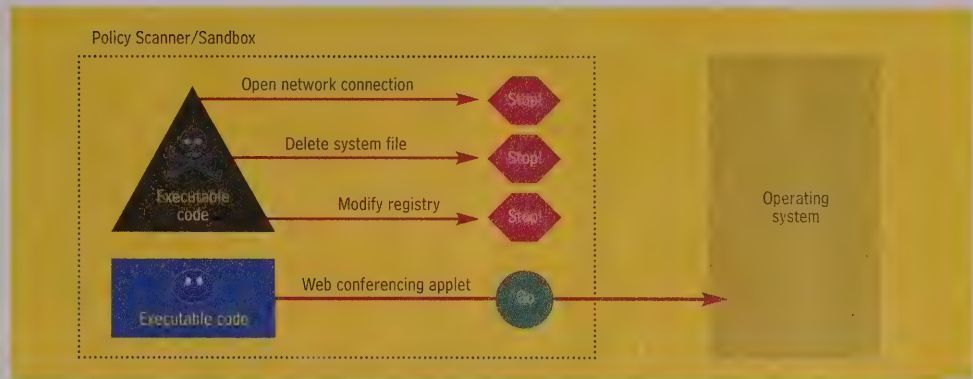


Figure 1. Behavior-blocking technology monitors executable code as it runs in real time. Any behaviors violating predefined policies are halted, and the code itself can be quarantined or killed. Non-malicious actions are allowed to proceed.

can be defined for groups, departments, and individuals.

SurfinGate for e-Mail scans both inbound and outbound SMTP traffic for naughty code, including Trojan Horses and scripts planted as attachments, inside .zip files, or in HTML e-mail. Code that violates a policy is blocked at the gateway or quarantined for later inspection. The current version of SurfinGate for e-Mail only allows for global policy creation.

You can deploy SurfinGate for e-Mail as an SMTP mail relay or as a plug-in for Microsoft Exchange 2000.

The gateway products run on Windows NT/2000 and Solaris 6,7, and 8. They are also available as appliances. SurfinGate and SurfinGate for e-Mail are available on an IBM eServer Series 330 box running Windows 2000. In addition, SurfinGate is available on a Sun Nexta x1 server running Solaris.

SurfinShield Corporate is installed on individual desktops. The software inserts itself near the kernel of the OS and monitors executables, ActiveX controls, Java applets, and Windows scripting hosts that arrive at the desktop via the Internet, e-mail, and Instant Messaging (IM).

If code attempts to open a network connection, delete or write files, access the system registry, or make OS calls, the desktop client acts and the code is sandboxed. Code that violates administrator-defined security policies is either halted or deleted. Finjan says the client software can surgically delete malicious code without interfering with any applications or Web browsers that might be running.

SurfinShield Corporate consists of a console component, a server component, and a client module. The console functions as an enterprise-wide mission control where policies are defined. The server holds those policies and maintains event

logs. The client agent enforces policies and sandboxes all executables. The client can run independent of the server, making it suitable for laptops that might be disconnected from the corporate network for extended periods of time. All three components run on Windows OSs.

Aladdin

Aladdin's (www.esafe.com) eSafe Gateway is a software-based solution that scans HTTP, FTP, and SMTP traffic for executable code, including Java, ActiveX, and scripting languages such as VBScript and JavaScript. As traffic passes through the eSafe Gateway, it sends that traffic to both the client that requested the traffic and to an inspection engine.

However, the gateway will withhold the final packet in the transmission from the client until the inspection engine has scanned executable code. If the scanned code is clean, the gateway completes the transmission to the end user. If the scanned code is malicious, the gateway alerts an administrator. The gateway also informs the end user that the transfer has been blocked.

The eSafe Gateway supports the Content Vectoring Protocol (CVP), which lets the gateway communicate with any OPSEC-compliant firewall and allows more targeted inspection capabilities. That is, the firewall will only pass potentially infectable files to the gateway for scanning. Noninfectable files, such as plain text or graphic images, are simply forwarded to their destination. The gateway can also communicate with OPSEC-compliant firewalls to request policy changes, such as allowing executable code to pass from trusted sources.

The gateway also includes a signature-based AV engine to block known viruses. The eSafe Gateway software runs on

Products Mentioned

Ataddin www.esafe.com

- eSafe Gateway, eSafe Enterprise

Finjan Software www.finjan.com

- SurfinGate, SurfinGate for E-mail, SurfinShield Corporate

Okena www.okena.com

- StormWatch

Pelican Security www.pelicansecurity.com

- SafeTNet

Tiny Software www.tinysoftware.com

- Personal Firewall 3.0 Network Edition

Trend Micro www.trendmicro.com

- InterScan AppletTrap

Windows NT/2000 servers. A specialized version integrates with Microsoft's Internet Security and Acceleration (ISA) server. The eSafe Gateway is also available as a Linux-based appliance for small and medium-sized organizations.

eSafe Enterprise sits on individual desktops and uses sandboxing and a personal firewall to thwart malicious code. The client software monitors each active process and application on the desktop via a system driver. The sandbox matches the executable code's behavior against an administrator-defined rule set and halts any action that violates that rule set.

The desktop client also functions as a personal firewall. Administrators can selectively block IP ports from being opened on the desktop. The desktop client also stops Trojan Horses that might have been inadvertently installed from opening ports to contact the attacker who installed the virus.

The eSafe client gives administrators substantial control over the user's machine. Administrators can lock users out of inappropriate Web sites (or restrict them to a set of trusted sites), block the use of certain words in e-mail, chat rooms, and Instant Messaging (IM), and stop users from reconfiguring the PC or installing software. The client also includes a signature-based AV engine to halt known viruses that find their way onto the PC.

Client agents are controlled from the eConsole, which configures, deploys, and manages those agents. Administrators can monitor security events from the console, adjust settings, and distribute network-, group-, or user-based policies.

The eSafe Enterprise client runs on Windows desktops. The console runs on either Windows NT/2000 or Novell Netware.

Pelican Security

Pelican Security's (www.pelicansecurity.com) SafeTNet is a desktop agent that monitors applications that can download executable code, including Web browsers, e-mail, Office applications, and chat clients. Whenever code is executed, SafeTNet's Dynamic Sandbox intercepts the system calls the code makes to the Windows OS. The sandbox checks these calls against a policy database, and acceptable system calls are allowed to proceed. Unacceptable calls, such as attempts to modify registry settings or open a network connection, are blocked. End users can't turn off or modify the SafeTNet client. The client can stop end users from downloading or installing unauthorized programs.

You can customize SafeTNet's out-of-the-box policies to allow particular processes to run, or you can create new policies to match the enterprise's needs. Administrators can apply policies globally or by groups, including groups already established in the enterprise via Windows NT.

SafeTNet has three components: the client agent, a server, and a management console. The server installs the client agent and sends policy updates. The client reports security events to the server. Administrators can manage those security events from the console. You can also integrate the product with management software, including UniCenter, HP OpenView, and Tivoli.

The client agent runs on Windows 95/98/NT, the server runs on Windows NT, and the management console runs on an NT workstation.

Trend Micro

The InterScan AppletTrap from Trend Micro is an HTTP proxy server that scans incoming Internet traffic for the presence of ActiveX, Java applets, and scripts. AppletTrap performs three checks on incoming mobile code. First, it looks for code with digital certificates; that is, ActiveX controls that have been digitally signed via Microsoft Authenticode, or Java applets containing digital certificates. Unsigned code, or code with signatures from unknown sources, can be blocked at the gateway.

Second, the product can block known malicious Java applets and JavaScript. Trend Micro maintains and continuously

updates a database of known malicious applets. Administrators can add to this database and also block any Java applets coming from blacklisted URLs.

Third, Java applets that pass the first two checks are wrapped in monitoring code at the proxy server and then transferred to the client. The client runs the applet in a sandbox. As the applet runs, the monitoring code checks its behavior against a list of administrator-defined policies. If the applet demonstrates malicious behavior, the monitoring code halts the action, notifies the user and administrator of the policy violation, and adds the applet to the database of malicious vandals. Applets that don't violate security policies are removed from the sandbox and allowed to run unimpeded. No client agent is required for this sandboxing function.

The proxy server runs on Windows NT/2000 and Solaris 2.6. The administration console uses Internet Explorer or Netscape Navigator for both local and remote access. AppletTrap runs as a standalone proxy or as a plug-in to Check Point's Firewall-1. It also integrates with other Trend Micro AV solutions.

Tiny Software

Tiny Software (www.tinysoftware.com) includes sandboxing functionality in its Personal Firewall 3.0 Network Edition. The sandbox throws up a barrier around ActiveX, Java, and other executables. It monitors the Windows registry, system services, system calls, file system, and IP ports. The sandbox prevents any actions that resemble administrator-defined malicious behavior, such as attempts to alter or delete particular files.

Administrators can configure and monitor personal firewall clients via a Windows NT/2000 domain controller. The client runs on the gamut of Microsoft OSs, from Windows 98 up to XP.

Okena

StormWatch, from Okena (www.okena.com), is a multifunction client agent that acts as a host-based IDS, personal firewall, and proactive worm and virus blocker. For instance, besides blocking the execution of malicious code, StormWatch can prevent port scanning and stop buffer overflows. StormWatch is available for both servers and desktops.

StormWatch deploys an agent that shims itself into the kernel of the host's OS, where it intercepts system calls in real time. The agent compares the system calls to predefined policies. System calls pointing

In theory, technology makes everything smarter. Reality is often a different matter. That is why each month, **Call Center Magazine** brings you the latest technology and trends in the customer care field—from site selection, to management and technology issues. Though nothing about shoe phones...yet.



Subscribe.
Free if you Qualify

IT MADE MAXWELL SMART

Products and Strategies for the Evolving Customer Interaction Center

Subscribe. www.callcentermagazine.com



CMP

United Business Media

CallCenter

Resources

For more information on server-based behavior-blocking products, check out "Web Server Lockdown," in the February 2002 issue of *Network Magazine*.

To read Carey Nachenberg's short paper, titled "Behavior Blocking: The Next Step in Anti-Virus Protection," go to <http://online.securityfocus.com/infocus/1557/>.

Worldwide Secure Content Management Revenue Share by Segment, 2000

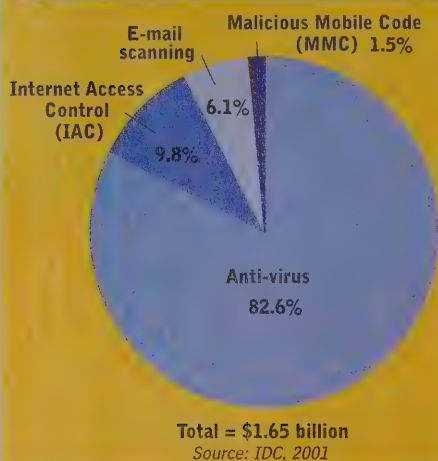


Figure 2. Traditional anti-virus companies, such as McAfee and Symantec, own the lion's share of the content-management market, according to analyst firm IDC. Behavior-blocking companies, which IDC labels Malicious Mobile Code (MMC), make up a trivial 1.5 percent. The remainder is divided between Internet Access Control (IAC) software and e-mail scanning.

to malicious or unwanted behavior (as defined by the policies) are blocked.

Rather than use a sandbox, the StormWatch agent simply monitors every application on the desktop. Four modules—the file interceptor, the network interceptor, the registry interceptor, and the COM interceptor—sit in front of the kernel to gather system calls. These interceptors coordinate with a rules engine to determine which actions are allowed and which should be denied.

A management console feeds policy updates to the rules engine. The rules engine then sends alerts and log data back to the console for analysis. StormWatch includes 12 out-of-the-box policies for a variety of applications, such as Microsoft

Office (including Outlook) and Instant Messenger. Administrators can also create customized policies.

The StormWatch desktop agent and management server run on Windows NT/2000. The management browser requires Internet Explorer 5 or Netscape 4.7x.

WHAT THE USERS SAY

According to several administrators using behavior-blocking products, the technology generally fulfills its function—catching unknown worms, viruses, and other malicious mobile code that AV signatures miss. Of course, they also noted several problems, including false positives, deployment hassles, and sometimes buggy products.

The security administrator at a major outdoor equipment and apparel company uses Finjan's SurfinShield desktop software on approximately 600 machines.

He was first attracted to the product by a rash of Outlook-based viruses. Although his company wasn't hit, he saw enough to convince him to seal a deal with Finjan. His experience with the behavior-blocking software has been mixed. "You can't underestimate the time and effort to get it out there."

He notes that false positives have been a problem, and not just with homegrown applications. "It doesn't play well with everything," he says. "It's not something you can just roll out without an impact."

On the other hand, he's also seen firsthand Finjan's protective capabilities. During a transition from Windows NT desktops to Windows 2000, the Goner virus struck. Several Windows 2000 machines, which hadn't been installed with Finjan's SurfinShield, fell victim to Goner. Windows NT machines running SurfinShield successfully repelled the virus.

The administrator says he'll continue to run SurfinShield in tandem with traditional AV software. He counts on behavior blocking to act as insurance against zero-day exploits, providing him some breathing room to apply more long-term fixes.

Tony Nelson is director of IT operations at StarPoint Solutions (www.starpoint.com), which designs digital business applications. He uses Aladdin's eSafe Enterprise and eSafe Gateway software to protect four Internet gateways and approximately 400 desktops.

Nelson sought out a proactive virus solution after the Melissa virus slipped into the network and shut down the New York office for a full day. Although he was

running anti-virus software, not all of his users had the latest updates.

His experience with eSafe has been positive. "The gateway catches 99 percent of our viruses," says Nelson. "The only time we find them on the desktop is when somebody has a laptop from out in the wild." He also likes the fact that end users can't turn off eSafe's desktop client or tamper with its settings. Despite eSafe's excellent track record, he has no plans to give up on signature-based AV. "I like having the dual vendor system. In today's times, you can't be too careful."

The security administrator for a large insurance company is using Okena's StormWatch on 500 desktops for remote employees who access the corporate network via the Internet. He uses the product as a personal firewall, but also appreciates its capacity to thwart unwanted code execution. "It's smart enough to know the difference between a system file and Nimda," he says.

He says he has been pleasantly surprised at how easy it is to configure and deploy policies. He also likes that it's invisible to end users and doesn't trouble them with lots of pop-ups and alerts, which in turn minimizes help-desk calls. "If they do run into trouble, [the agent] logs back to a master console and I can monitor that," he says. "Then I can change the policy and distribute it back to the folks that are connected."

THE NEW FACE OF ANTI-VIRUS SOFTWARE

Some experts see behavior blocking as the wave of the future, a wave that will wash away signature-based AV products. After all, if the blockers you've installed successfully catch both known and unknown threats, why bother running a second, unnecessary layer of software—especially if all it does is demand updates and generate subscription fees?

It's a good question, and the answer has two components. The first is economic. In terms of market share, behavior-blocking software is a ripple, not a wave. Companies making behavior-blocking software own 1.5 percent of the market, according to a report from research firm IDC (see Figure 2). By contrast, AV companies own nearly 83 percent. (The remainder belongs to e-mail scanning and Internet access control software.)

Even though IDC predicts that behavior blocking will grow faster than standard AV software (29 percent compound annual growth vs. 14 percent compound annual

growth), AV vendors will still be sitting on an estimated \$2.7 billion market in 2005; the behavior blockers won't even crack \$90 million. Thus, it's unlikely that traditional AV companies will dry up any time soon.

Second, a major appeal of traditional AV technology is its certainty. Digital fingerprints clearly identify viruses, and the AV software removes it without fuss. That means network administrators don't have to spend time constructing detailed mobile code policies, examining quarantined code for malicious intent, or explaining to irate vice presidents why Web apps keep shorting out. In addition, AV technology can also clean out infected systems, a feature that no behavior blocker can match.

The upshot is that signature-based anti-virus solutions aren't going away. Still, traditional AV vendors would be foolish to ignore behavior blocking (ever hear of David and Goliath?), because they can't escape the fact that their current methods are ineffective against the new breed of blended threats.

What's likely to happen is the major vendors will use their market dominance to absorb, Borg-like, the behavior blockers,

either through partnerships, acquisitions, or by developing their own blocking technology.

AV market leader McAfee has already begun this process. In November 2001, it launched a partnership with Finjan to integrate McAfee's anti-virus scanning engine into Finjan's product line. In April 2002, Aladdin announced a partnership with Kaspersky Labs that offers Kaspersky's anti-virus module to eSafe customers.

Symantec has also hinted that it's pursuing a behavior-blocking strategy. In March 2002, Carey Nachenberg, chief architect of Symantec's security response team, published a paper entitled "Behavior Blocking: The Next Step in Anti-Virus Protection" on the SecurityFocus.com Web site (see Resources). While the paper doesn't directly state that the company is developing a behavior-blocking product, it indicates that Symantec is thinking hard about the future of AV technology.

Trend Micro is launching a service, known as the Outbreak Commander, that uses policy-based behavior-blocking to shorten the gap between the appearance of virus and the creation and distribution of signatures. When Trend Micro obtains a virus or worm sample, it writes a policy

specifically geared to identify and halt any malicious behaviors.

For example, during a recent worm outbreak, Trend Micro engineers had a policy ready for customers in just 20 minutes; by comparison, the full signature took nearly an hour to develop. This is a clever use of policy-based behavior blocking, and it greatly reduces the window of vulnerability; however, it is not a truly proactive mechanism because customers must still wait for Outbreak Commander to acquire a virus or worm sample and make updates available.

And as for administrators, it would be unwise to give up anti-virus signatures, but perhaps just as unwise not to investigate behavior blocking. As new threats continue to evade standard defenses, behavior blocking offers a proactive solution to zero-day exploits. The time you spend fine-tuning behavioral policies and weeding out false positives will be well worth seeing unknown malicious code bounced from your network, hours before the first AV signature arrives at your inbox. Suddenly, the race is fair again. *

Andrew Conry-Murray, business editor, can be reached at amurray@cmp.com.

Simplify your life.



Thanks to Net to Net's Ethernet DSL, you still can.

Net to Net Technologies, DSL the Easy Way™

As easy as



Net to Net's Ethernet-based DSL solutions can be deployed in a fraction of the time, and at a fraction of the cost, of traditional ATM-based DSL systems. Net to Net has a DSL solution to fit every deployment scenario, whether it's ADSL, SHDSL, VoDSL or T1, from the Central Office or the Remote Terminal. The IP services your customers desire, such as high-speed Internet, multicast video, and interactive gaming are all supported over an end-to-end IP network. That means your network just got a whole lot better, and your life just got a whole lot easier.



www.NetToNet.com contact@NetToNet.com

Tel 603.427.0600; 877.638.2638 (toll free) Fax 603.422.0610

112 Corporate Dr., Pease Intl. Tradeport, Portsmouth, NH 03801

Network Security Options Making you Dizzy?

attend **NETSEC 2002**

TECHNICAL DIMENSIONS OF NETWORK SECURITY

Reserve your
place today!

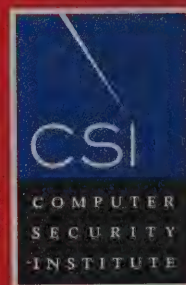


SAN FRANCISCO

JUNE 17-19, 2002

HYATT REGENCY EMBARCADERO

For more information go to www.gocsi.com,
phone 415.947.6320 or email csi@cmp.com



www.gocsi.com

FEATURING

INTRODUCTORY TRACK, SECURE E-COMMERCE, INTERNET/INTRANET
SECURITY, VPNS, REMOTE ACCESS, TELECOMMUNICATIONS, CRYPT-
TOGRAPHY, COMPUTER CRIME, INTRUSION DETECTION & FORENSICS,
MANAGEMENT AWARENESS INTRO, CISSP EXAM PREP AND MUCH MOR

SECURITY:

Reducing Risk in an Imperfect World



In a perfect world, hackers wouldn't write viruses. Employees wouldn't snoop into confidential records. And no one would ever lose a laptop.

But it's not a perfect world. Malice and carelessness create a growing range of threats, making information security ever more complex and challenging. To make matters worse, security resources are often very limited. Security requires money, personnel, and processing power. None of these are in infinite supply.

So technology managers must answer some tough questions: Where can I most effectively spend my security dollars? How can I optimize security without hiring more staff? How do I implement new security measures without adversely affecting the performance of critical services?

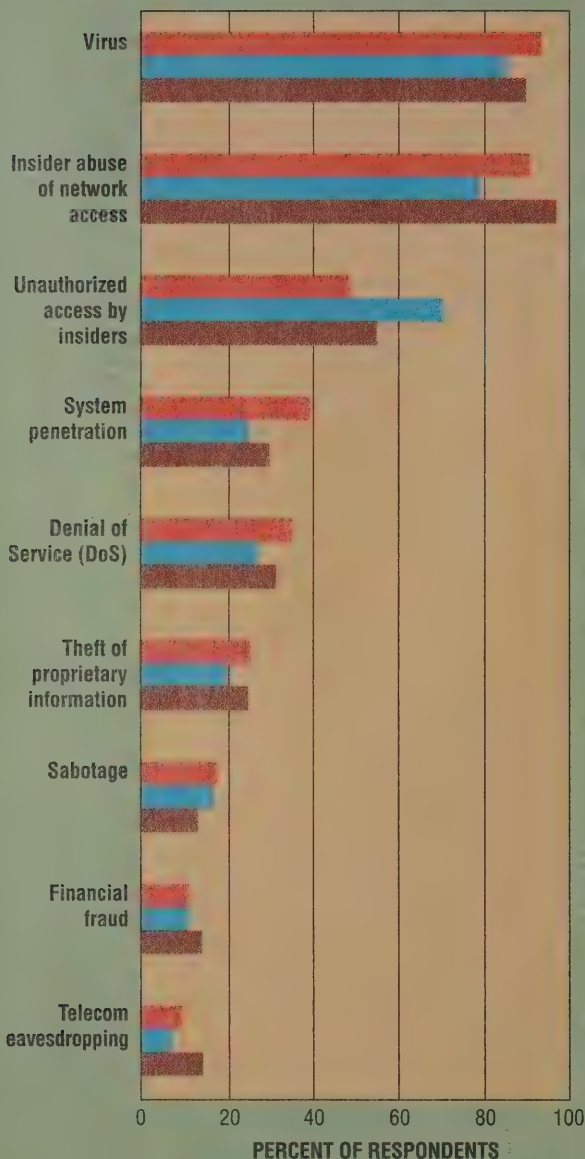
To answer these questions, network managers must carefully evaluate risks and remedies. Otherwise, they can run out of resources before this imperfect world runs out of dangers.

NETWORK MANAGERS

can easily spend all their time and money putting locks on every door and window—only to wind up leaving the key under the mat where anyone can find it.

Assorted Attacks

What types of cybercrimes has your company experienced?



2001
2000
1999

Base: 484 respondents in 2001
583 respondents in 2000
460 respondents in 1999

Data: FBI/CSI Computer Crime and Security Survey of Computer Security Practitioners

WHERE'S THE RISK?

One of the main mistakes that network managers make is failing to understand where their companies are most exposed to real risk. One reason for this is that the computer industry, by its very nature, generally focuses on security issues for which vendors sell products—not the ones that may represent the greatest economic threat to individual businesses.

For example, lots of people will discuss the strength of network encryption technologies and how to best protect data traveling over a public wire. In reality, however, the chance of valuable corporate data being stolen in transit is slim to none. By contrast, the loss and theft of laptops—which often hold extremely valuable information—is a daily occurrence. Yet few organizations encrypt laptop drives as a matter of policy.

“Most IT departments fail to fully and accurately identify their assets,” claims Russ Cooper, who bears the title of “Surgeon General” at TruSecure Corporation because of his role in educating the public about threats to computing health. “They therefore don’t adequately focus on effectively protecting access to those assets and as a result, leave themselves unacceptably exposed.”

Cooper provides another laptop-related example. Companies go to great lengths—and can spend a lot of money—to keep viruses off their network, scanning e-mails and installing anti-virus software on every desktop. Then along comes a laptop user who’s picked up an infection while dialing into the Internet at home. The user then plugs into a corporate LAN and before you know it, there’s a major outbreak.

“Using anti-virus software is a little like getting into your car and putting on a seat belt,” says Cooper. “It’s an absolutely essential precaution, but it doesn’t mean that you’re now so invulnerable that you can drive however you want to and still not get hurt.”

Cooper suggests that, rather than relying entirely on anti-virus software to keep malicious code out of the enterprise, organizations do a better job of securing their perimeters with content filtering gateways. These solutions prevent undesirable content from coming into the enterprise environment at all, reducing or eliminating the need to find and isolate viruses on networked PCs and servers.

THE INDUSTRY

generally focuses on security issues for which vendors sell products—not the ones that may represent the greatest economic threat to individual businesses.

SAFE PASSAGE

SONICWALL



When it comes to moving money through rough neighborhoods, safe passage is defined by this bank vault on wheels. When it comes to moving information across the Internet, safe passage is defined by SonicWALL.

Safe passage requires a balance of hardened security and rapid delivery of your valuable information. That balance is achieved by SonicWALL's comprehensive line of firewall and VPN appliances coupled with a complete portfolio of security applications such as Network Anti-Virus, Content Filtering, and Strong Authentication. SonicWALL's award-winning Global Management System makes your distributed security infrastructure easy to deploy and easy to manage.

SonicWALL's security solutions keep your valuable information rolling through the Internet's roughest neighborhoods—safe and sound.

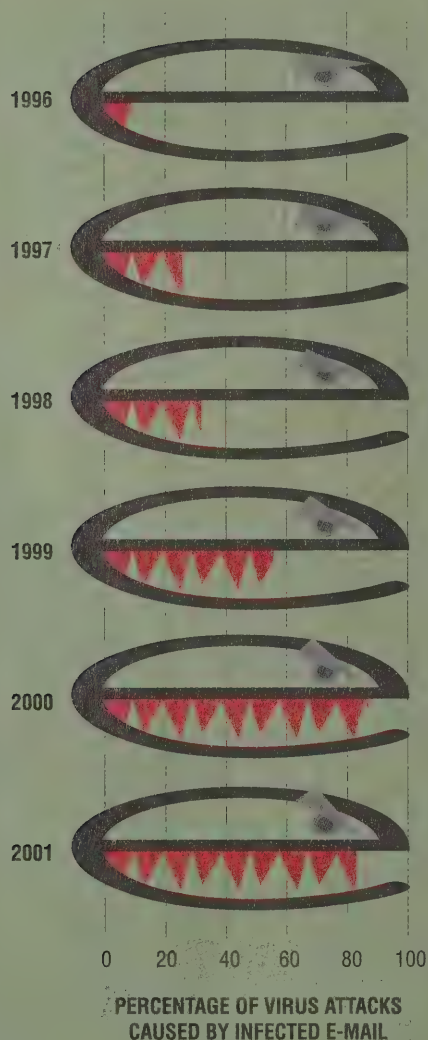
To find out more about how SonicWALL Internet security appliances can deliver cost-effective, hardened firewall security for your network, visit <http://www.sonicwall.com/network>, or call SonicWALL at 888-557-6642 or 408-745-9600.

COMPREHENSIVE INTERNET SECURITY



The changing face of malicious code

Once upon a time, floppy disks were the primary source of virus infections. Now, as the chart below indicates, e-mail is the main point of exposure.



Source: ICSA.

"Firewalls only let you decide which services to allow through your Internet connection," notes Cooper. "But you have to think past the services and also give yourself the ability to keep out specific types of content, such as cookies that contain scripts."

FOREIGN POLICY

When it comes to firewalls themselves, Cooper advises taking a "default deny" approach—for example, starting with all services turned off and only opening those that are proven necessary for business. This takes firewall management beyond the purely technical sphere and into the realm of business management.

"If somebody wants you to open up the firewall for NetMeeting, for example, they should be challenged to develop a business case for doing so," says Cooper. "If they can't justify the value to business, then the network manager shouldn't have to expose the company to additional risk by enabling another service."

UNFORTUNATELY,
network managers may ignore
the protection of a particularly
pivotal asset, such as an
executive's desktop browser

Network managers can't stop at what they let *in* through the firewall and e-mail servers; they also have to be concerned about what they let *out*. Many security threats have been known to hijack corporate resources and use them to infect other organizations. In addition to causing damage to other organizations, these incidents can also jeopardize business relationships that generate revenue and marketshare.

Unfortunately, network managers may ignore the protection of a particularly pivotal asset, such as an executive's desktop browser. An attacker can then use that browser to make the executive appear to do just about anything. If any of these tamperings reach a business partner—or, worse yet, is visible to the larger public—it can have devastating consequences for the company's reputation.

The interconnectedness of today's e-business environment has all kinds of potential consequences. For example, network managers are careful to craft VPN solutions that ensure the security of communications between the enterprise network and specific trusted parties. But they don't really take any measures to ensure that those trusted parties are really trustworthy. That is, VPN technology itself doesn't provide any mechanisms to ensure that the trusted client is actually free of malicious code itself, or that it isn't under the control of some "untrusted" third party. Security managers must therefore consider taking measures to evaluate the security of partners' systems before establishing VPN connections.

power

performance

security

ease-of-use

centralized management

real-time analysis

support

No eye candy, bells or whistles...no hype, glamour or tricks.

Sourcefire brings peace of mind to enterprises by combining the best of breed Snort IDS with an easy-to-use interface, a management console for distributed environments and a full support staff to alleviate your worries.

Sourcefire means enterprise intrusion detection...plain and simple.

correlation

customization

award-winning

scalability

flexibility

manageability

attack detection



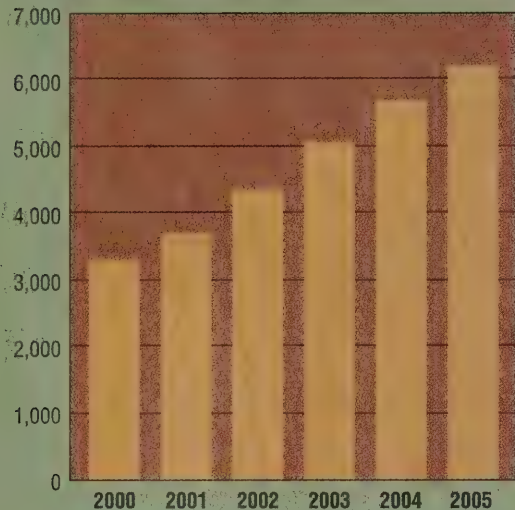
From the creators of the original Snort IDS

www.sourcefire.com

info@sourcefire.com

Worldwide Security Software Revenue Forecast

MILLIONS OF DOLLARS



Source: Gartner Dataquest (November 2001)

Security managers also have to be careful that, in their ardor to improve security, they don't actually make matters worse. Password rotation is a perfect example of this phenomenon. Over-zealous managers may insist on having users change their passwords frequently to safeguard corporate systems. But overly frequent password changes may in fact force users to write their passwords down. This can create a greater risk of unauthorized access than a good, strong password that's been used for a few months.

It's also easy for managers to spend money on security tools that don't do much. For example, many companies have implemented Single Sign-On (SSO) systems in an effort to consolidate authentication of multiple enterprise resources. What they don't realize is that users may already be using the same password for all those resources, so the investment doesn't really pay off in added protection.

COUNTING THE COST

With so many different vulnerabilities to consider and so many different security technologies available to address those vulnerabilities, many network managers are looking for a good strategy for prioritizing security spending. The security industry has been debating the issue of investment metrics for some time, since conventional Return on Investment (ROI) calculations obviously don't apply to security spending, which focuses on loss prevention rather than revenue generation and productivity.

One metric that's starting to gain acceptance is "Reduced Risk on Investment," or RROI. With RROI formulas, security investments are ranked based on the amount of risk they reduce per dollar spent, with risk calculated by multiplying potential financial loss by the probability of an incident occurring.

In more graphical terms:

$$\text{RROI} = \frac{\text{Potential loss} \times (\text{Probability without expenditure} - \text{Probability with expenditure})}{\text{Total expenditure}}$$

By applying this formula, various alternative security investments can be prioritized based on their projected business value. For example, a \$25,000 piece of software that can reduce the chance of a company leaving itself open to a million-dollar privacy lawsuit from 50:1 to 500:1 would wind up with a score of 0.72. By comparison, assigning \$10,000's worth of person-hours to address a security issue that affects three out of four companies and has a downside risk of only about \$50,000 scores a healthy 1.25—even if it still leaves a 50 percent chance of the incident occurring.

The outcome of such RROI calculations may seem counter-intuitive to managers who fear the \$1,000,000 consequence more than the smaller one. But risk is governed as much by probability as it is by raw dollars, and very high-end long-shot risks are often more cost-efficiently offset by insurance policies than by technology.

NETWORK SECURITY DON'T COMPROMISE



CYBERGUARD'S FIREWALL/VPN IS
AN INTEGRATED, FULL-FEATURED,
EASY-TO-MANAGE
SECURITY SOLUTION.



Defend your domain with the first firewall appliance
to achieve the EAL4 Certification. CyberGuard, the
technology leader in network security.

U.S.: 954-958-3900
Asia: 954-958-3878
Europe: +44 (0)1344 382550
e-mail: info@cyberguard.com
For more information visit:
www.cyberguard.com

CYBERGUARDTM
WORLDWIDE
DEFEND YOUR DOMAIN

Copyright 2002 CyberGuard Corporation. All rights reserved.

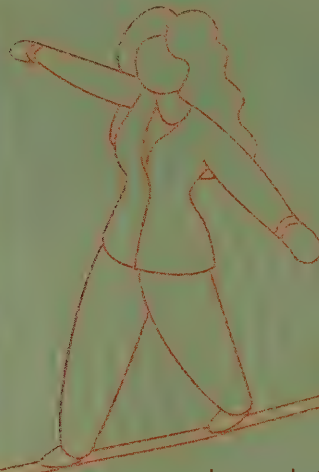
MSPs: LOCKING THE BACK DOOR

A special case of trusted relationships involves managed network services and Management Service Providers (MSPs), which put the responsibility for the operation of all or part of the network in an outsider's hands. These outside organizations are placed in a particularly sensitive position of trust, since they're given direct access to critical infrastructure assets.

The question for network managers is how to ensure that 1) the MSP won't inadvertently expose his or her company to a threat by a lack of diligence in its own security implementation, and 2) that access to network elements is effectively restricted to the authorized MSP.

This access control is typically accomplished by using network-based authentication technologies, such as Remote Authentication Dial-In User Service (RADIUS) servers. This creates a bit of a problem because MSPs never need access more than when there's a problem on the network. Unfortunately, if the network is down, network-based security controls won't do much good because the connectivity between MSP-managed elements and those controls will likely be lost.

The solution in such situations is to safeguard critical managed network elements with access control devices of their own. These inexpensive single-port devices contain their own authentication database and can even be designed to work with security tokens for maximum protection. They can also be used to enable and secure out-of-band network management (that is, management of devices via dial-up connection rather than over the corporate LAN/WAN), which also provides essential remote access to critical devices in the event of network failure.



In order to make such calculations, however, information security managers need to know what kinds of threats are real and which ones are just hype. That's why decision-makers are so hungry for credible security statistics. It's also why security audits are so valuable: They point out exactly which threats have the highest probability of hurting the company, and therefore help determine where to best spend security dollars for maximum immediate benefit.

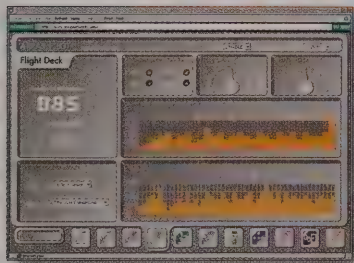
When network managers engage a security consultancy to do an audit, they're actually seeking a form of education. They want to learn where they're vulnerable and what they can do about it. By the same token, they're often advised to become educators themselves—teaching users to be safer about how they access the network and its resources. Educated users are one of the best defenses against threats ranging from laptop theft to social engineering.

VERY HIGH-END
long-shot risks are often
more cost-efficiently
offset by insurance
policies than by
technology

Just as important as educating users, however, is educating executives. After all, the best way to overcome a security budget shortfall is to get a bigger budget. And that's only going to happen when technology managers become more adept at presenting security vulnerabilities to upper management in terms of dollars and cents. Without that funding, businesses will find that the same information technologies that give them a business edge also expose them to an unacceptable range of business risks.



First we directed traffic... Now we police it!



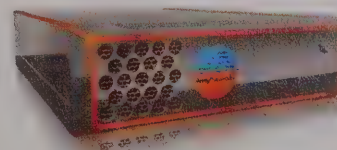
Network security gets graphic. ArraySP delivers a flight deck full of controls and monitors in the form of an ultra-friendly GUI. So say goodbye to command line languages and hello to point-and-click policing.

Array Networks®
Power tools for the Web

Our initial product line delivers highly integrated platforms for optimizing web traffic performance. Array Networks is now pleased to introduce the simple solution for managing user access with uncompromising security: The Array SP (Array Security Proxy). The Array SP polices your web-based network from end-to-end. This plug-and-play device puts a robust stack of security solutions between your users and the enterprise's precious network resources. Integration doesn't require the complex software installations that tend to devour IT

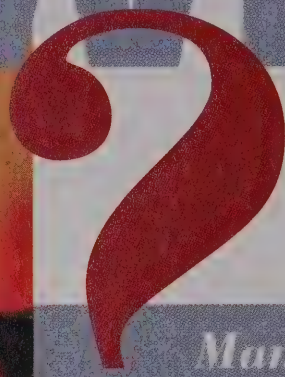
budgets and infinite hours. For day-to-day control and monitoring, you'll find the interface remarkably intuitive and simple.

If you want to know more about the pain-free way to protect your network, call 1-866-MY-ARRAY, visit www.arraynetworks.net/nm



Product specifications are subject to change without prior notice.

Manage My What



Managed Security Services

Sponsored by:

Array Networks®
Power tools for the Web

CYBERGARD™
WORLDWIDE
DEFEND YOUR DOMAIN

SONICWALL

sourcefire

Outsourcing your network's security to a Managed Security Service Provider might be just the answer you are looking for, but it involves technical, financial, and policy issues that need resolution before you sign a contract.

So, to that end, *Network Magazine* is hosting a "Customer and Service Provider Views of Managed Security Services" panel discussion and luncheon at

SUPERCOMM 2002

When: Wednesday, June 5th 2002

Time: 12pm - 1:30pm

Where: Georgia World Congress Center,
Rm B-312

*And we'd like you to attend, **FREE.***

To RSVP please go to

www.networkmagazine.com/securityevent



CMP
United Business Media

Network Magazine

Ultra-Wideband Wireless: Fat Pipes from Thin Air?

UWB doesn't break the laws of physics, but it's an exciting technology—and it could even live up to Bluetooth's hype.

by Andy Dornan

Up until now, you couldn't take the phrase "mobile Internet" literally. Whether describing the slimmed-down, text-only services available through a smart phone or full-scale wireless Web surfing, mobile Internet has really meant mobile access to the Internet.

If current tests of Ultra-Wideband (UWB) technology are successful, we could soon see the real thing: tiny routers embedded in every electronic device, and eventually other objects, from pens to business cards. Before that comes to pass, though, we'll probably see high data rate wireless LANs (WLANs), several times faster than current IEEE 802.11 networks. The target speed, already demonstrated in the labs of vendors such as Intel and Xtreme-Spectrum (www.xtremespectrum.com), is around 100mbits/sec—real throughput, and not shared between multiple users. Perhaps more importantly, these high data rate WLANs could have battery lives measured in years, rather than hours.

Of course, this comes at a price. Despite what some proponents of UWB might claim, the amount of data that can be sent over the airwaves is still finite. Unrestricted UWB transmissions could interfere with current radio spectrum users, cutting into the bandwidth of existing wireless, and even fiber, networks. Because UWB is also touted for other applications, from personal radar to surveillance systems, its widespread use could even mean a loss of available capacity for voice and data networking.

Because of such fears, regulators have been reluctant to allow UWB. So far, the FCC has permitted only four companies to manufacture and sell UWB devices, and none of the devices are intended for communications. Three make imaging systems, aimed at construction and safety

personnel. The fourth product, and the only one sold to the public, is a "toilet ventilation device."

That changes this month, as new regulations announced in February 2002 come into force. Peer-to-peer UWB is limited to low power and is still only allowed on an experimental basis, but the industry has high hopes. The tight restrictions could ultimately result in better systems that use airwaves more efficiently, and with such low energy requirements they won't need batteries or power cords.

SURFING WITHOUT WAVES

The most extreme hype around UWB claims that it uses no radio spectrum, and

that it eliminates radio's traditional reliance on waves in favor of short pulses. The first claim is simply wrong: UWB uses more spectrum than other radio systems, hence the name. The second claim is only partially true. All networking technologies, wireless or otherwise, are based on electromagnetic waves, and UWB is no exception. It does, however, abandon the concept of a carrier wave, meaning a specific frequency to which radios must be tuned.

Instead, UWB broadcasts on many frequencies simultaneously, distributing its signal across a vast bandwidth. This is similar to spread spectrum, the basis of 802.11b WLANs and Code Division Multiple Access (CDMA) cell phones use, but UWB spreads a signal over a wider band—potentially across the entire radio spectrum, though no government would permit this. The FCC, the only regulator that allows UWB communications systems at all, has initially restricted them to a bandwidth of 7.5GHz (see table on page 68). That's hardly infinite, but still many times broader than the spectrum allocated to every other networking system combined.

The huge bandwidth requirement means UWB can't be given a dedicated part of the spectrum in the same way as most wireless technologies. (Even unlicensed systems, such as WLANs, are still confined within a relatively narrow frequency range.) UWB must instead share

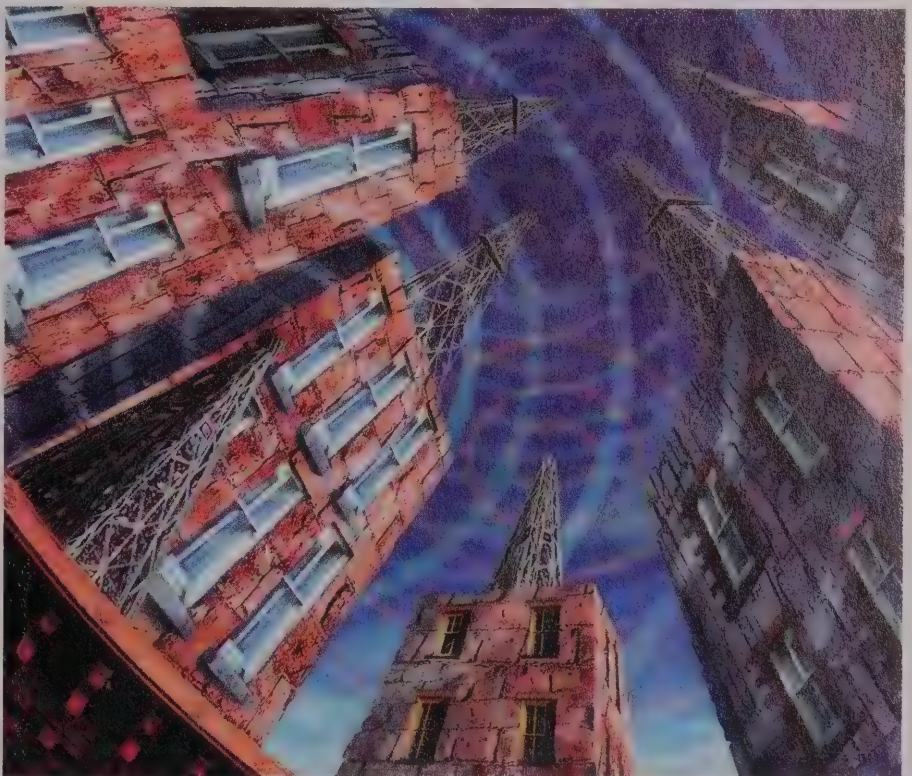


Illustration: David Ball

Spectral Bandwidth of Wireless Data Technologies

System	Bandwidth Used	Regulatory Control in U.S.
AMPS or D-AMPS (1G or 2G cellular)	0.03 MHz	Licensed spectrum
GSM (2G cellular)	0.2 MHz	Licensed spectrum
IS-54 CDMA (2G or 3G cellular)	1.25 MHz	Licensed spectrum
Wideband CDMA (3G cellular)	5 MHz	Licensed spectrum
IEEE 802.11a or 802.11b (wireless LAN)	25 MHz	Confined to ISM or U-NII band
UWB (communications type)	7500 MHz	Power restricted by Part 15 rules

Bandwidth Bandit? Ultra-Wideband is so-called because it spreads its signal over a very wide band of frequencies. It requires so much that it can't have a dedicated portion of the spectrum, instead broadcasting at low power in bands already used for other purposes.

the airwaves already allocated to other systems. This reuse of existing bandwidth leads to claims that UWB provides something for nothing. The theory is that because the signal is so thinly spread over so many frequencies, the amount of interference it causes at any one frequency should be negligible.

Naturally, existing radio spectrum users don't see things that way. When the FCC first announced that it was considering allowing UWB transmissions, it received thousands of pages of comments, mostly from companies, user groups, and even other federal agencies worried about interference. Broadcasters, airlines, radio hams, astronomers, and the military are all concerned that UWB's gain could be their loss.

UWB proponents say low power interference already occurs at many frequencies, permitted by the FCC's Part 15 rules. These rules are intended to allow devices such as computer processors, which inadvertently act as transmitters at their clock frequency—currently anywhere from about 300MHz to 2GHz, which encompasses most of the bands used by broadcasting and cellular services.

UWB transmitters would stay within the limits set by the Part 15 rules, but actually transmit useful information. There is already a precedent for this, in the form of amateur broadcasting: Anyone in the United States can set up an unlicensed radio station, provided it keeps within the Part 15 rules. The rules are quite strict, limiting the effective range to about 100 meters, or 300 feet—impractical for most types of broadcasting, but not for a WLAN.

This argument doesn't convince existing spectrum users. Most existing Part 15 devices transmit in only a small part of the spectrum, whereas UWB needs to cover a

wider bandwidth. Although UWB's power at any particular frequency might be within limits, its overall output could be higher than that of a Pentium chip or even a Part 15 radio station. Users are also concerned about the sheer number of UWB devices that might eventually be produced, each of which could add a little more interference.

UWB's strongest critics are in the cell phone industry. Sprint PCS (www.sprintpcs.com) was the most aggressive, because its network is based entirely on CDMA, the cellular technology most susceptible to interference. On the basis of tests conducted jointly with UWB company Time Domain (www.timedomain.com), Sprint claimed that widespread use of UWB would reduce its network capacity by up to 1,000 people at busy periods in a typical city—even if each UWB device were restricted to an output power only 6 percent of the Part 15 limit. It also threatened to sue the FCC for breach of contract.

Other cell phone companies also attacked UWB, because they all hope to upgrade their networks to some form of CDMA. Cingular even claimed that UWB could interfere with pacemakers and hospital equipment. In a January 2002 letter to the FCC, the United States's four largest mobile operators—AT&T Wireless, Cingular, Sprint, and Verizon—and the CDMA patent-holder Qualcomm jointly warned that, "People in an office building trying to use their cell phones to report a fire or other emergency could well have their calls blocked if there are UWB devices operating on a nearby local area network."

ULTRA-WIDE BANNED

It's easy to be suspicious of cell phone companies' motives. They could be

attempting to use concerns about interference to shut down a competing technology, rather than simply ensure that their own technology continues to work. Sprint wouldn't comment on this, but its filings with the FCC have claimed that the UWB companies "want to use Sprint PCS's spectrum for free to provide telecommunications services in competition with Sprint PCS's services."

The distinction might seem arcane, but it's important legally. Cellular operators have paid billions for licenses entitling them to use a certain part of the radio spectrum, so they have a legitimate reason to be upset if others are causing interference in "their" bandwidth. These licenses do *not* entitle them to a monopoly over wireless voice and data services, however. In North America, and increasingly in other countries (See "Europe Warms to Hotspots," page 26), anyone can offer a service in the freely-available spectrum used by WLANs. Though this might upset cellular operators, an attempt to shut down these operators would simply be anti-competitive.

The FCC eventually dismissed most of the cellular operators' concerns about interference, at least with the voice signal itself. It said that Sprint's tests were conducted in ideal lab conditions that didn't correspond to the real world and pointed out that people experiencing interference could simply move a UWB device away from a cell phone, or switch it off entirely. The cell phone companies disagree, saying that customers expect their cell phones to work everywhere and are likely to blame the service provider, rather than their own UWB devices, when calls are dropped.

Even if UWB doesn't interfere with the voice or data signals, cellular operators have another legitimate reason to be worried: the Global Positioning System (GPS). The GPS also uses CDMA, and because its signals are transmitted from satellites, they can be extremely weak by the time they reach users. Potential interference with the GPS signal is also what upset the military and the airline industry, which now depends on the GPS to route almost all flights within North America.

Cell phone networks rely on the GPS signal in two ways. First, the narrowband CDMA systems used in the Americas and some parts of Asia require the GPS to synchronize the clocks at their base stations. The networks would fail completely if the GPS signal was jammed, but this is unlikely. Most base stations are in areas

with a clear view of the sky, making the signal easier to pick up. They're also fenced off to protect people from their radiation, simultaneously protecting the station from UWB or other potentially disrupting Part 15 devices.

More worrying, the FCC's Enhanced 911 (E-911) mandate requires all U.S. carriers to track their users' location, and the most accurate way to do this is to build a GPS receiver into every phone. Because cell phones have to work indoors and get a fix quickly, their receivers are often more sensitive to the GPS signal than the stand-alone GPS devices used by hikers, aircraft, and even the military.

This extra sensitivity (achieved through updates sent over the cellular network) also makes the cell phone's GPS receivers more vulnerable to interference, though exactly how vulnerable has yet to be determined. Qualcomm (www.qualcomm.com), the largest vendor of these enhanced GPS systems, has warned that its technology simply won't meet the level of accuracy required by E-911, if a wideband Part 15 device is nearby. However, UWB vendor xTremeSpectrum claims that it can build UWB and GPS into the same device without interference problems.

The FCC is worried about the effect of UWB on GPS, so has heavily restricted UWB communications within the GPS band—to a level about 0.04 percent of that allowed for other Part 15 devices, which it says should be below the regular background noise level. (See Figure 1.) It's also restricted UWB communications within other bands, including those used by cell phones, though not by as much, and by amounts that vary based on the type of UWB device.

Within a building, UWB can transmit at up to the same level as the Sprint tests (6 percent of the Part 15 limit). Outside, they're limited to one-tenth of that, because walls and other obstacles inside help to dampen the signal. Higher power levels are allowed for some other purposes, including imaging, but these levels are already attracting criticism as too low.

Although UWB is often touted as revolutionary, this only applies to its applications in communications. As far as imaging is concerned, a similar system called ground-penetrating radar (GPR) has been used for over 40 years by miners, archaeologists, Apollo astronauts, and anyone who needs to see underground. Most recently, it's been used in laying and repairing fiber cables, which, unlike their copper predecessors, are invisible to metal

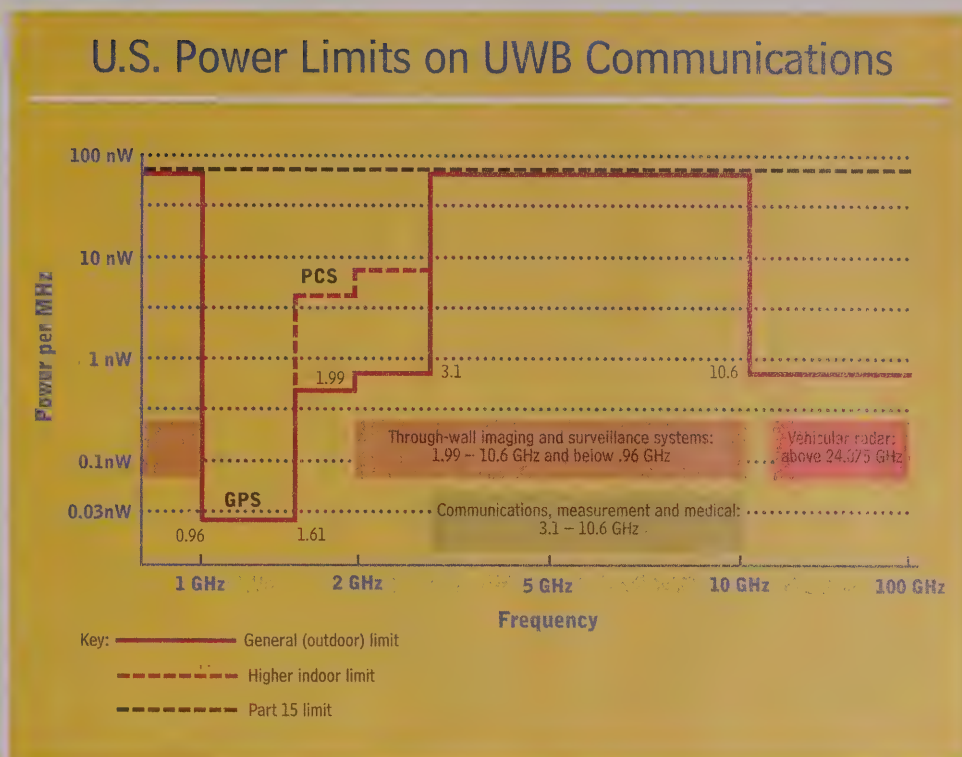


Figure 1. The FCC permits three main types of UWB transmission. Communications equipment is allowed to transmit at up to the same power level as other Part 15 devices within its designated band, but must maintain strict limits at other frequencies. These limits are less strict for indoor than outdoor use, because walls help to dampen the signal.

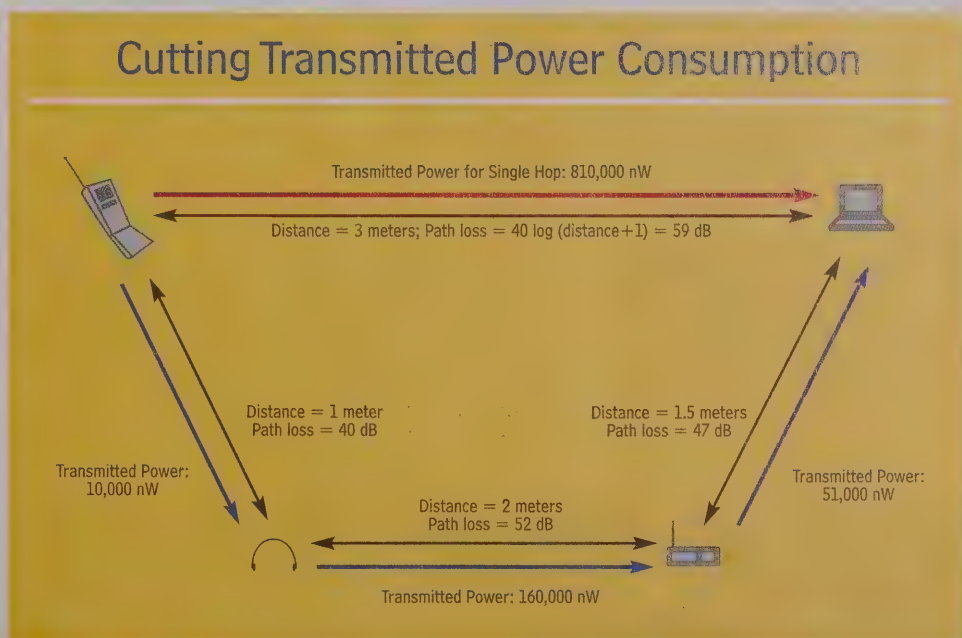


Figure 2. The most direct route between two devices is often not the most efficient. In this example, the computer needs to receive a signal of at least one nW, and signal strength varies with the inverse fourth power of distance. A cell phone three meters away would need to transmit a signal with a power of 810,000 nW to cover this distance. By routing the signal via chips embedded in two other household devices, the system uses a total power of only 221,000 nW. (Decibels can't simply be added, so the total path loss of the three together is about 54 dB.) Even though the signal travels further and uses two extra routing hops, power consumption is reduced by more than two thirds.

Resources

Ultra-Wideband (UWB) vendor Multispectral Solutions has a useful and (by vendor standards) unbiased FAQ covering the technology at www.multispectral.com/uwbfaq.html.

Æther Wire & Location has produced an entire CD-ROM filled with PDF format papers, some technical, covering the history and applications of UWB. Much of the material is also available online, at www.aetherwire.com/CDROM/General/papers.html.

The Berkeley Wireless Research Center, at <http://bwrc.eecs.berkeley.edu>, runs the "PicoRadio" project, which aims to develop short-range wireless data networks with low power consumption.

The FCC's February 14, 2001 decision on UWB, along with PowerPoint slides and statements from commissioners, can be seen at www.fcc.gov/Bureaus/Engineering_Technology/News_Releases/2002/nret0203.html. All of the comments the FCC received from cellular operators, UWB vendors, Global Positioning System (GPS) users, and other interested parties have also been posted online, in PDF format. They are accessible via a Web form at http://gulfoss2.fcc.gov/prod/ecfs/comsrch_v2.cgi, which requires the FCC proceeding number ("98-153").

A good overview of the theory and tests results for and against UWB's interference with GPS is in the September 2001 issue of *GPS World* magazine, posted online at www.gpsworld.com.

For an explanation of how UWB works, see *Network Magazine's* tutorial (Lesson 160: Ultra-Wideband Wireless Networks") in the November 2001 issue on page 30. We also have more on GPS, Enhanced-911 (E-911), and location technology. See "Can M-Commerce Find a Place in Your Network" on page 38 of the same issue, and "Did Cell Phones Save the White House?" December 2001 on page 78. All are available online at www.networkmagazine.com.

detectors. Despite relatively high energy levels, it hasn't caused any interference problems for wireless networks, because most of this energy is directed into the ground.

GPR now falls under the same rules as newer UWB systems, causing an uproar among its existing users. Since the regulations were first announced, almost every comment sent to the FCC has been from a GPR service provider or user, warning of dire consequences if it's banned. Among other things, they say that a GPR ban could

lead to an increase in the "backhoe problem," when someone digging into the ground accidentally cuts through a piece of fiber and causes a network outage.

FREE BANDWIDTH, FREE ENERGY?

Because of the FCC's different rules for indoor and outdoor UWB networks, two different types of devices are likely to emerge. The regulations say that the more powerful devices, intended for indoor use only, will need a mechanism preventing them being taken outside. The most obvious such mechanism is a power cord (with no battery), which seems to negate the main advantage of a wireless system, but might not make it entirely pointless. Many consumer devices do spend most of their lives plugged into wall: For example, UWB could stream video from a VCR to several TVs around a home.

Devices designed for outdoor use are more interesting. Many of these will probably be used indoors too, but need to meet the stricter outdoor interference requirements, because they'll work in "untheatred" mode. Their low power means they're likely to have a short range, more like a much faster version of the Bluetooth Personal Area Networking (PAN) technology than a full-scale WLAN. Indeed, the IEEE's 802.15 working group, which studies wireless PANS, is considering UWB as the Physical layer for a future standard. The current standard, 802.15.1, is almost identical to Bluetooth, but the IEEE wants future versions to offer a higher data rate or lower energy consumption.

UWB can achieve both of these goals, thanks to the way it generates a signal. Instead of using complicated modulation schemes and antennas, it emits staccato pulses of white noise directly from a chip. The gaps between pulses are much longer than the pulses themselves, so for most of the time the system is idle. Coupled with the FCC's restrictions on output power, this could enable a device to run for months between battery charges.

There's even research into eliminating the battery altogether, instead relying on "energy scavenging," which extracts tiny amounts of energy from the environment as needed. For example, a wearable UWB transmitter might be able to harness the energy generated when a person moves, as some "self-winding" watches already do.

There isn't much energy available for scavenging, so a batteryless wireless system might need to reduce its power even further. The most efficient way to do this could be to send a transmission via several

short routing hops, rather than a single longer one. This is because the received signal strength in an indoor environment falls off rapidly as a transmitter and receiver move further apart, often by a factor proportional to the third or fourth power of distance. Even what appears to be a roundabout route can use less energy than the direct path.

This is the wireless version of peer-to-peer distributed computing. Whereas the peer-to-peer systems currently deployed across the Internet distribute storage (Napster) or processing (Web services), this would distribute routing. Every node would act as a router, automatically passing packets along the most energy-efficient path. (See Figure 2 on page 69.) This vision does have some weaknesses: The more links in a chain, the more likely it is to be broken by devices moving too far apart. And the most efficient path is one that reduces the distance between nodes to zero, otherwise known as a wire.

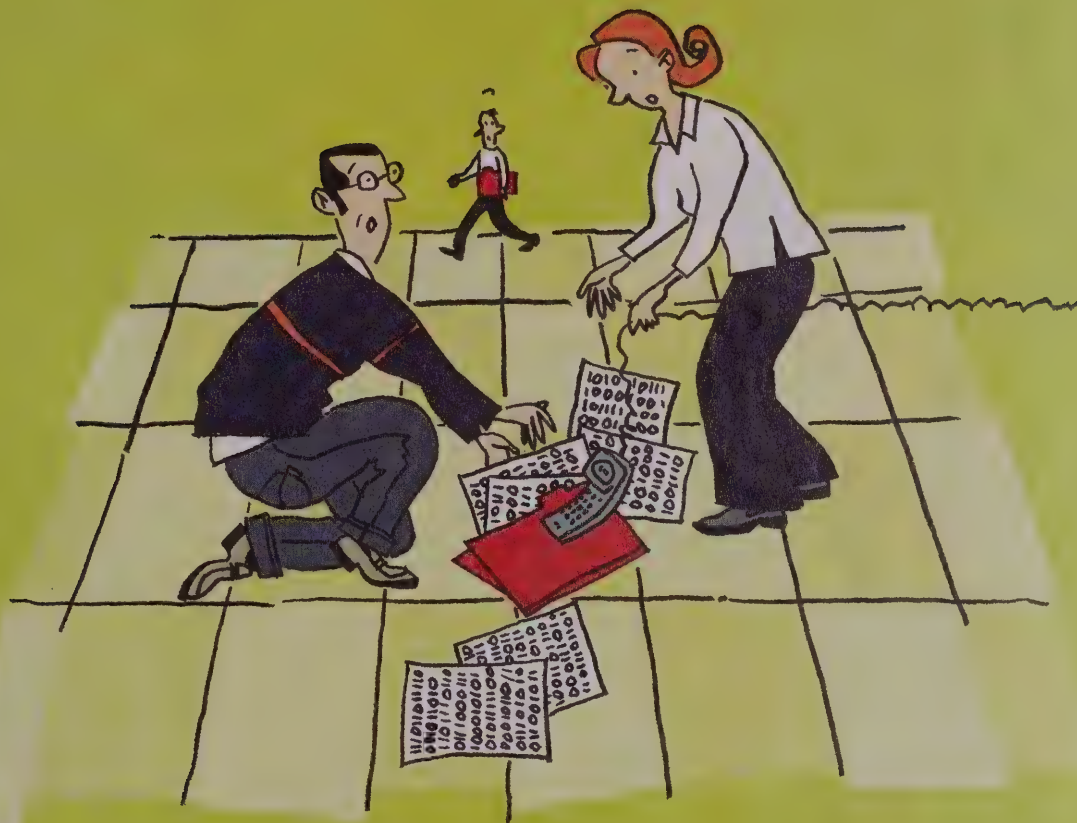
Energy scavenging networks probably won't have high data rates, but more conventionally powered UWB transmitters promise 100mbits/sec or more. A UWB network's data rate is proportional to the number of pulses per second, so in theory it can scale with the chip speed. Some vendors even describe UWB as "Moore's Law Radio," saying its performance could double every year or two.

Such claims are probably over-optimistic, and UWB will still run up against limits. (See "How Vendors Use Math to Lie," page 86). Moving pulses closer together makes them more susceptible to multipath interference, a problem from which UWB is so far immune. Other interference issues are likely when several UWB devices are close together and transmitting at the same time. But even without any increase, UWB's demonstrated speed already matches the fastest WLANs.

That isn't a fair comparison, because WLANs are available now and UWB is still theoretical. But we don't have long to wait. Vendors are rushing to get products out of the labs, and XtremeSpectrum says that it will ship a chipset aimed at consumer gadgets by the end of June 2002. We should soon find out whether the hype is justified. *

Senior editor Andy Dornan's new edition of his book, *The Essential Guide to Wireless Communications Applications*, ISBN 013-0097-187, is published by Prentice Hall. He can be reached at adornan@cmp.com.

Hey! You got voice in my data!



You got data in my voice!

REDEFINING TELECOM

Subscribe to *Communications Convergence* and each month receive strategic guidance, lab-tested product information, case studies on successfully deployed convergence solutions, and industry news and analysis. **We make sure good ideas aren't misplaced, suppressed, or ignored in the noise.**

Communications Convergence. Redefining Telecom. Subscribe.

Free if You Qualify. www.ccmagazine.com



CMP

United Business Media

COMMUNICATIONS
CONVERGENCE

Emerging from the dotcom shakeout with profits, Hoover's Online ensures 24-by-7 uptime after deploying application-tracking software.

by Jim Carr

Hoover's Online Keeps Its Subscribers Online All Day, Every Day

By its own account, Hoover's Inc. is the "home page of the corporate world." Hoover's, which offers both free and fee-based information about businesses, marketplaces, people, and products to three million users worldwide, might be overselling itself a bit—after all, thousands of Web sites offer similar, business-focused information.

However, the Austin, TX-based Hoover's Online (www.hoovers.com) division has emerged from the dotcom shakeout in fine fettle. With paid subscriptions accounting for about 70 percent of its \$30.1 million in 2001 revenues and sales nearly doubling from year to year since 1999, Hoover's finally turned a profit at the end of 2001—a considerable accomplishment for a mostly online media company in decidedly down economic times.

That success hasn't come without growing pains. Hoover's had to close two subsidiaries—content syndicator Hoover's Media Technologies (formerly Powerize) and its European operations—and abandon its Web site focused on careers, business travel, and personal finance.

Through it all, Hoover's, founded in 1990 as The Reference Press and renamed Hoover's in 1996, has continued to meet its core audience's key demand: delivering dynamically updated corporate information. This core audience consists of sales, marketing, business development professionals, and senior-level executives, all looking for that bit of data to give them an edge over rivals. Because Hoover's provides its content solely in English, most

clients are in the United States and Europe, with some in the Pacific Rim.

With information on more than 12 million public and private companies, including 19,000 in-depth profiles written by the company's 90-member editorial staff, keeping the site current and online isn't for the faint of heart. This daunting task belongs to Bill Chambers, the company's systems manager and the man responsible for keeping Hoover's content up and available all day, every day.

Chambers and his staff recently turned to an application- and performance-management product from a small, privately held Silicon Valley start-up to handle the task of staying online all the time. The software, ProactiveNet from ProactiveNet Inc. (www.proactivenet.com), provides tools to manage the performance of line-of-business applications and their associated infrastructure.

This article looks at how application-management products like ProactiveNet can help online businesses such as Hoover develop an early warning system to significantly reduce an organization's mean time to recover from systems failures.

NO TIME TO WASTE

As networks and the types of traffic they carry have become more complex, the need for management tools combining infrastructure and application-monitoring capabilities has expanded dramatically. IT managers are realizing they can't waste their resources tracking problems caused by unknown software or hardware failures.

"If we could get the world to agree on what performance management is, then it would be number two [behind security] in the minds of IT executives," says Michael Dortch, a principal analyst with market consultancy the Robert Francis Group (www.rfgonline.com).

Dortch says that managing application performance has become the Holy Grail to enterprise IT personnel, because without it, you have no useful tools to enforce Service Level Agreements [SLAs] or to demonstrate delivery of business benefits from investment in IT resources. "You either have to make or save money—preferably, both—and it's an IT department's job in a nutshell to do that," Dortch adds. That's where performance-management software tools such as ProactiveNet come in.

ProactiveNet is one of many such products that have popped up in the market over the last couple of years. Others include Agilent's (www.agilent.com) Firehunter, Altaworks's (www.altaworks.com) Panorama (see "Altaworks's Panorama," August 2001, page 32), Computer Associates's (www.ca.com) Unicenter, and Dirig Software's (www.dirig.com) RelyENT (see "Dirig Software's RelyENT, xSPress, and Fenway," September 2001, page 28).

John McConnell, a principal analyst with McConnell Associates (www.mcconnell.com), says the market for performance-management software is growing in the 20 percent to 30 percent range annually. This growth comes as no surprise to McConnell and Dortch.

Bill Chambers, Hoover's systems manager, has moved the online business to a new application performance-management solution that has reduced the time it takes to resolve problems while allowing him to make better decisions about network upgrades.



Business Profile

HOOVER'S INC.



Headquarters: Austin, TX

Web address: www.hoovers.com

Industries: Online information delivery

Project leader: Bill Chambers, systems manager

Technology in focus: Application performance-management software

Size: 2001 revenue of approximately \$30.8 million, 287 employees

Business challenge: With three million subscribers worldwide accessing Hoover's Online information on more than 12 million public and private companies, as well as 19,000 in-depth profiles written by the company's editorial staff, the company needs to keep its online business applications running 24-by-7. Subscribers can access Hoover's proprietary editorial content through a variety of channels, including Hoover's Online, Hoover's Business Press, and the company's CD-ROM products. The channels also include outside distribution partners such as America Online, Bloomberg, Factiva, Fortune, LEXIS-NEXIS, CNBC on MSN Money, The Washington Post, and corporate intranets.

A hodgepodge of free and homegrown monitoring tools, all poorly integrated, provided insufficient information on the performance of Hoover's applications.

Solution: Hoover's Online implemented an application- and performance-management product from ProactiveNet, a privately held start-up. ProactiveNet's software gives online enterprises the tools to manage the performance of line-of-business applications and their associated infrastructure.

ProactiveNet's built-in intelligence enables it to recognize regular surges in traffic loads at specified times of the day, when Hoover's Online subscribers access key information. This has led to about a 50 percent reduction in the time it takes Hoover's to resolve problems. The software also provides information allowing Hoover's Online to make better-informed decisions about adding new hardware or software resources to its data center. *

Concerns over the ability to guarantee application availability is "what's keeping a lot of IT executives awake at night," says Dortch. Justifying spending is difficult for most IT personnel, he explains, and performance-management tools can pinpoint where specific problems are occurring and need attention. The performance-management products also take over where the large systems-management products, such as Hewlett-Packard's OpenView or IBM's Tivoli (www.tivoli.com), leave off, says McConnell. These monitoring and reporting tools lack the fine-tuned granularity of the performance-management applications, he says.

One key capability of ProactiveNet, for instance, is its ability to track average peaks and valleys in an application's operation, notes Chambers. "ProactiveNet has intelligence built into it, so it knows that at 9 a.m., I [always] see a big rise in people logging into the system. It learns to recognize there will always be an increase then, and thus won't send a problem alert," Chambers says.

Enterprise Systems Management Software (SMS) can't react in those ways, according to McConnell. "It's an entirely different type of product," he says, pointing to two other distinctions between the two products.

One is deployment time. A typical HP OpenView or Tivoli deployment takes nearly a year. Installing ProactiveNet is simpler. McConnell says the ProactiveNet customers he's surveyed have reported installing and deploying the product in a day or less. Chambers concurs, noting that a team of ProactiveNet sales engineers got his systems up and running on several test machines in mere minutes. Within 24 hours, his staff could deploy ProactiveNet on other servers Hoover's wanted to monitor at initial deployment.

The second distinction is consulting and integration expenses. With SMS systems, enterprises can easily spend \$50,000 on consulting, in addition to software costs. ProactiveNet offers a host of features, easy to use and deploy, and requiring little outside help, according to McConnell.

ProactiveNet CEO Ajay Singh also notes that SMS products focus more on network root cause problems, not applications-related issues. For example, he says if a port on a router goes down, an SMS system would report that the servers connected to it appeared to be down as well. In this situation, the SMS can't communicate with the servers to discover whether

they're up or not, and reports them as being down, which isn't the case. A performance-management product diagnoses the reasons why an application's transaction response times have degraded. It doesn't focus on network-related issues, Singh adds.

DISTILLING DATA

Designed specifically to monitor application transactions and identify the root cause of application-transaction slowdowns, ProactiveNet analyzes large volumes of data collected from across the enterprise-application infrastructure, including applications, transactions, URLs, databases, network devices, firewalls, and servers.

With dozens of systems and millions of applications transactions, the typical online business generates huge amounts of collectible performance data. For instance, an application server tracks up/down status, what applications are running, processor and memory use, disk space available, and logical connections. These are just a few of the hundreds of possible variables. Multiply that by dozens of computers running multiple applications, and the IT personnel monitoring those systems can be overloaded with information.

ProactiveNet uses a patented statistical-analysis algorithm to filter through these variables, drilling down to the root cause of degraded transaction processing. According to ProactiveNet, the software narrows the potential causes of a problem down to a manageable few, so users can pinpoint the root cause, predict problems, and initiate problem resolution before a problem actually disrupts online applications or services.

By putting the information collected through its statistical-analysis tools, ProactiveNet can calculate a normal operating envelope for every performance variable the product tracks. ProactiveNet can pin down the operational parameters for what is normal for a particular time of day, such as Monday at 8 a.m., on the weekend, or at night.

The result is "a bubbling up of the abnormality linked to the root problem," Singh says. This capability allows ProactiveNet users to operate within so-called intelligent thresholds, or dynamically changing utilization points indicating when an application or process is stressed.

With these techniques, ProactiveNet's software can cut an online business's mean time to recovery from a problem by

29th Annual Computer Security Conference and Exhibition



November 11 - 13, 2002

CHICAGO

Hilton Chicago Towers

Over 130 Sessions—Topics Include:

- Network Attacks and Countermeasures
- Windows NT Security
- Secure Web Commerce
- Computer Crime
- DDOS Attacks
- Intrusion Detection and Response
- Cryptography
- Hackers
- Computer Forensics
- Managed Service Providers
- PKI
- VPNs and Firewalls
- Security Awareness
- Selling Security to Management
- Policies and Procedures
- Internet/Intranet
-and much more!



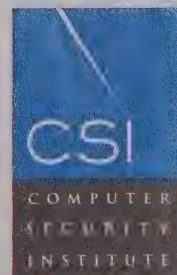
Yes!

Please send conference catalog upon publication.

Fax to 415.947.6023, phone 415.947.6320 or email csi@cmp.com

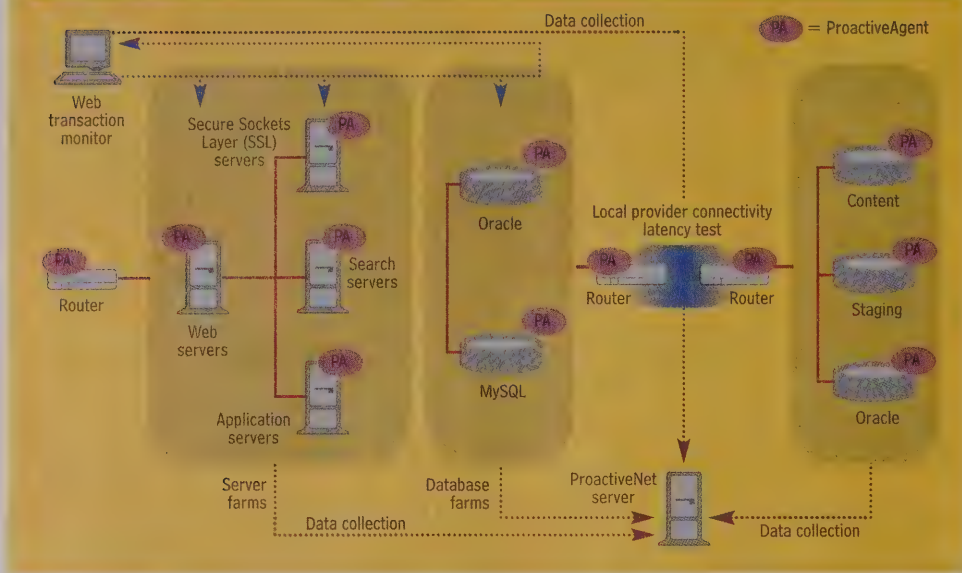
Name _____
Company _____
Address _____
City • State • Zip _____
Country _____
Phone _____ Fax _____
Email _____

For information on exhibiting call Cynthia Deno at 831.335.9445 or email cdeno@cmp.com



Find updated
conference information at
www.gocsi.com

Hoover's Online Transaction Network



Tracking Trouble. The Hoover's Online transaction systems, including the company's servers and its dual database applications, are monitored by a performance-management console from ProactiveNet. Loaded onto each key network component—routers as well as servers—is a ProactiveAgent (PA), which collects data on that system's operations. The data collected is fed to the ProactiveNet Web transaction monitor, which looks for traffic spikes and anomalies and reports problems to the ProactiveNet server.

a factor of five to ten, according to the company. Moreover, by reducing the number of IT personnel dedicated to problem resolution, the product can increase profits by eliminating infrastructure-related costs.

MINIMALLY INVASIVE AGENTS

Like most performance-management products, ProactiveNet requires running software agents on the device being monitored. These agents collect specific data on applications and servers, then forward the data to ProactiveNet's monitoring console, which users can integrate into several of the SMS systems, such as HP's OpenView.

ProactiveNet says it has prebuilt Java-based agents for about 50 Windows NT/2000, Unix (including AIX), and Linux applications, covering about 80 percent of the systems and applications found in most data centers. These include the Apache (www.apache.org) and Microsoft IIS Web servers, the iPlanet (www.iplanet.com), BroadVision (www.broadvision.com), and ATG Dynamo (www.atg.com) application servers, and database systems from Oracle, Sybase (www.sybase.com), Informix (www.informix.com), and Microsoft.

"Our objective is to be as minimally invasive as possible in our data collection,"

explains Singh. He notes that ProactiveNet's agents consume less than one percent of a CPU's capacity.

ProactiveNet says it differs from other products in this category in its ability to accept data from a customer's proprietary agents. The company's Meta-API, or monitor wizard, enables users to easily integrate homegrown monitoring scripts into the ProactiveNet environment. This ability allows ProactiveNet customers to continue using proprietary reports generated by their own agents alongside the product's reporting capabilities.

ProactiveNet can also collect and filter data collected by most high-end SMS systems, including those from Computer Associates, BMC (www.bmc.com), and IBM's Tivoli (www.tivoli.com) division. ProactiveNet uses agent adaptors to do this, which literally adapt data from the SMS products for interpretation by ProactiveNet. These adaptors translate information collected by third-party and homegrown monitoring agents into a format the ProactiveNet software can read.

A 3 A.M. START

The first wave of traffic hits the Hoover's Online Web site at about 3 a.m. CST each day, when London-based companies open for business. Executives and sales people

begin logging into Hoover's, looking for information on the companies they'll be doing business with that morning, explains Chambers.

That's the first of several traffic spikes to hit Hoover's IT resources in a typical working day. Activity on the Hoover's Online site really begins to heat up about 8 a.m. CST, when folks on the Eastern seaboard start turning on their PCs. A second series of bumps hit the site after lunch, as subscribers begin planning for their afternoon meetings.

It's up to Chambers and his staff of six systems personnel to ensure problems don't negatively impact the computing resources where Hoover's runs its Web-based business during these key times. Among these resources are an assortment of Unix- and Linux-based servers from Sun Microsystems, Penguin Computing (www.penguincomputing.com), and VA Linux Systems (www.valinux.com). The company also uses various Unix and Linux applications, including BEA Systems's (www.beasys.com) iPlanet application server, Vignette's (www.vignette.com) v6 Content Suite content-management software, and Oracle and the open source (www.mysql.com) databases.

If these systems fail, so might Hoover's subscribers, who rely on the site to gather business-critical information about potential customers, partners, and competitors. "There's no room for downtime, in our opinion," Chambers says. And with subscribers in all time zones across the globe, "we have to be up 24-by-7, and I want to know if anything unusual is happening [on the site] during those bumps."

The challenge of keeping these resources up and available 24-by-7 is daunting. Not only is the Hoover's Online database system extensive—for competitive reasons, Chambers declines to reveal its exact specifications—it's also changing constantly as company profiles are added and updated, companies bought and sold, and executives move up or down the corporate ladder.

Until a year ago, Chambers and his staff relied on what he calls a hodgepodge of freeware, third-party, and homegrown monitoring tools to track the company's Web-based resources, most of which are located at an Austin data center operated by Inflow (www.inflow.com), an application and managed services provider.

Dissatisfied with that combination of software, Chambers says he began a quest in March 2001 to consolidate the monitoring tools the company uses. "I wanted a

way to present [systems performance] information to the technical staff in one easy-to-read format," he says.

That task was complicated. "One of the problems I ran into from the beginning was that the outside monitoring services, such as Keynote Systems [www.keynote.com] and Gomez Advisors [www.gomez.com], could tell me how fast a page [loaded] where they put their nodes up, but they didn't tell me what happened inside my firewall," Chambers says. "When Gomez says that our page delivery is slow at 3 p.m., it doesn't mean our systems are slow—it could be a problem in the Internet.

"What I wanted was something to tell me how fast I was generating pages or performing a task, but didn't show the impact of outside influences, such as bandwidth bottlenecks, bad routers, or peering points," says Chambers. ProactiveNet allowed him to correlate data collected internally with the performance metrics from the outside agency to get a clearer picture of where problems were.

"ProactiveNet not only tells us how our systems are running, but has intelligence built in that helps it learn to recognize there will always be an increase in traffic at certain times of the day," says Chambers. This puts the product ahead of most monitoring tools, which require setting hard-and-fast maximum and minimum load thresholds and force users to put the threshold above their daily peaks, according to Chambers.

ProactiveNet learns to follow those peaks as the norm and alerts operators to inconsistencies within the normal operations cycle. Therefore, Hoover's has a lower tolerance threshold for problems and faces fewer alerts, with more realistic threshold, which leads to better management of the company's Web resources.

Chambers looked at 15 vendors, both large and small, and was struck by ProactiveNet's small footprint on the machines it monitors. ProactiveNet consumes few of the PC's resources, so it doesn't degrade performance, which often occurs when using a software-based agent to monitor system operations.

The initial ProactiveNet test deployment went off without a hitch. ProactiveNet sales engineer Rob Morrison handled installation via a remote telnet session, and the Hoover's staff added several servers to the environment the next day.

Hoover's put ProactiveNet into full production in early January 2002 and now monitors about 30 to 40 systems with it.

Hoover's uses ProactiveNet to collect server I/O information, memory and CPU utilization statistics, Ping times (which indicate latency), and numerous variables within the Oracle and MySQL databases. Hoover's Online systems staff now benefits from consolidated monitoring, true alerting of abnormal conditions, and the ability to identify those conditions in a more expedient manner, says Chambers.

While the ProactiveNet software hasn't labeled any of Hoover's applications as "bad citizens," it did turn up one problem early on. ProactiveNet showed that one of Hoover's applications was making too many database calls simultaneously, which locked out other applications intermittently, making it difficult for Chambers and his staff to pinpoint where the problem was. "By collecting data on the application and looking at ProactiveNet reports, we could see what the culprit was," Chambers says.

Chambers and his staff challenge the ProactiveNet software regularly by purposely breaking nonproduction systems. For instance, they'll overload a database or change a server's port settings. "Anything to throw a monkey wrench in when we can. We haven't been able to beat it yet," he says.

The product also allows him to set up and deliver custom-tailored reports for different levels of personnel at Hoover's. These reports eliminate what Chambers calls "management alarms," which occur when an executive's friend calls to complain about slow downloads from the company Web site.

With these nontechnical reports, Chambers can show his executives that an apparent problem wasn't with Hoover's systems, but with the friend's Internet connection. "The reality is, people always believe [poor performance] is a Web site problem, and not the thousands of miles of fiber between them," Chambers says.

The software's built-in reporting capabilities also give Chambers the information he needs to make budgetary and planning decisions, such as adding new hardware or software. By showing trends in Web-site characteristics, such as page-generation times and response thresholds, ProactiveNet can determine when a company needs to add resources, such as a new

Web server or database application, according to Hoover's systems manager.

For bottom-line purists, Chambers says ProactiveNet has cut problem-resolution time by 50 percent, and he thinks that figure can be improved with better understanding of the product. The result is better and more effective use of systems personnel.

LOOKING AHEAD

Despite the fact its product performs as promised, ProactiveNet still isn't a slam-

dunk to succeed, according to RFG's Dortch. As a privately held, venture-funded start-up, it faces an uphill battle to win market share.

Dortch thinks ProactiveNet probably has no more than 12 months to gain sufficient traction to survive in a competitive market niche. The best way to do that is via partnerships.

Partnerships are especially important if ProactiveNet wants to sell into large enterprises. IT executives in these organizations want to do business with companies that will be around for a while, and with companies

whose technology plays with others, according to Dortch.

That's why ProactiveNet's integration into HP's OpenView and its relationship with Keynote Systems are important to many potential customers. On one hand, the integration with OpenView allows running ProactiveNet within the OpenView environment, giving systems managers at large enterprises a consolidated view of their network hardware resources and transactional performance.

On the other hand, ProactiveNet's software complements Keynote's services, which deliver performance-management measurement of Internet-based transactions to online businesses. Together, the two can give an e-business an end-to-end look at the performance of transactions on its site.

With that kind of information in hand, online businesses such as Hoover's can stick to the job they do best: dishing up business-critical Web pages to millions of busy customers around the world. *

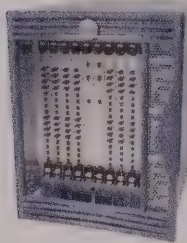
Jim Carr is an Aptos, CA, freelance business and technology writer. He can be reached at jecarr13@charter.net.

ProactiveNet cut problem-resolution time by 50 percent, and that figure can be improved with better understanding of the product.

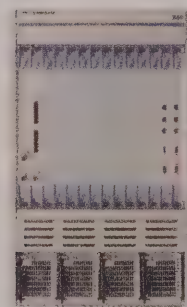
New Products & Services

Brocade Introduces New 2Gbit/sec Fibre Channel Switch
GFI's MailSecurity Scans E-Mail with Multiple Virus Engines
AT&T Enhances VoIP Suite

by the *Network Magazine* staff



The SilkWorm 12000 Core Fabric Switch from Brocade is a 2Gbit/sec Fibre Channel switch.



Crossbeam Systems' X40S appliance runs multiple security software on one box.



AirMagnet's Handheld analyzes wireless protocols on a palmtop.

HARDWARE

Brocade Introduces New 2Gbit/sec Fibre Channel Switch

Brocade's new SilkWorm 12000 Core Fabric Switch is a 2Gbit/sec Fibre Channel-based system available in 64- and 128-port configurations. The system has a modular bladed architecture, and includes 128 ports in a 14-rack units enclosure, which helps to optimize space utilization. The system provides dual redundant fabrics, and has hot-swappable components, including switch modules, redundant power supplies, processors, and cooling systems.

Storage Area Network (SAN) management capabilities are included in Brocade's Intelligent Fabric Services platform, which can be accompanied by API-enabled third-party storage management applications. The SilkWorm 12000 provides forward and backward compatibility with the other switches in the SilkWorm line. The product can be extended to support up to 10Gbit/sec Fibre Channel as well as future IP-based and InfiniBand protocols.

The street price of the SilkWorm 12000 system is expected to range from under \$150,000 to over \$200,000.

Brocade, 1745 Technology Dr., San Jose, CA 95110, (408) 487-8000, www.brocade.com.

Crossbeam System Puts Best-of-Breed Security Software on One Appliance

The x40S 2.0 from Crossbeam Systems is a hardware appliance that can run concurrent security solutions from top vendors, including Check Point's Firewall-1 and VPN-1 and Enterasys Network's Dragon Sensor Intrusion Detection System (IDS). Crossbeam also plans to announce partnerships with security vendors in the anti-virus and Denial of Service (DOS) markets.

Targeted at enterprises and data centers, the x40S replaces the need for multiple servers and appliances to run individual security applications. The product comes with a pair of network processor modules, a pair of control processor modules, and up to 10 application-processing modules to run the security software. Add-on

cards for IPSec and Secure Sockets Layer (SSL) encryption/decryption are available to accelerate performance. The appliance can also be configured with up to two Gigabit Ethernet interfaces or 16 10/100Mbit/sec interfaces.

Crossbeam Systems says the x40S achieves five-nines availability. Two appliances can be configured for high availability. The box also includes mirrored hard drives and redundant interfaces, power, and fans. Administrators manage the box via a GUI, and remote management options include Secure Shell (SSH), HTTPS, and SNMP traps.

Pricing for Crossbeam's x40S 2.0 starts at \$52,600.

Crossbeam Systems, 200 Baker Ave., Concord, MA 01742, (978) 318-7500, www.crossbeamsys.com.

Wireless Protocol Analyzer in an iPaq

AirMagnet's Handheld is the first pocket-sized packet sniffer and network-planning tool for Wireless LANs (WLANs) based on the Wi-Fi (IEEE 802.11b) standard. It consists of a PC or CF+ Card that plugs into any palmtop running Windows CE 3.0 (Pocket PC 2002), and includes AirMagnet's Wireless System Expert (WISE) software for both Windows CE and Windows 2000. This helps to integrate the data it gathers into other Windows applications.

The Handheld understands all 802.11b protocols and can identify every node on every possible 802.11b channel. This means it can easily detect war driving (outside hackers trying to access the network), rogue access points (set up by other departments without IT approval), access point impersonation (MAC address spoofing), and poorly configured encryption. It can also optimize the physical architecture and channel use of a complex network, detecting sources of interference such as microwave ovens.

The AirMagnet Handheld card costs \$2,495, including software. It also requires a Windows CE palmtop, which will add about \$600 to the price.

AirMagnet, 707 Koa Ct., Sunnyvale, CA 94086, (888) 828-3773, www.airmagnet.com.

ADIC Tape Libraries Revved Up to 2Gbits/sec

ADIC's Scalar tape libraries have been upgraded to a 2Gbit/sec Fibre Channel interface. This includes the Scalar 100, Scalar 1000, and Scalar 10k automated tape library systems. Supporting from one to more than 600 tape drives and from 15 to more than 15,000 cartridges, the systems were designed for environments ranging from workgroups to large enterprise data centers. The 2Gbit/sec upgrade is a follow-on to the company's initial introduction of systems that support the 2Gbit/sec interface.

The Scalar 100 is a midrange system that supports up to eight drives and 96 tapes. The system provides up to 25Tbytes of capacity in 14 rack units. The Scalar 1000 supports up to 48 drives and up to 1,182 tapes. The Scalar 10k supports up to 648 drives and 15,885 cartridges, and has a total native capacity of up to 1,588Tbytes.

The systems support Linear Tape Open (LTO), SuperDLT (SDLT), and Advanced Intelligent Tape (AIT) technologies.

Pricing for the systems starts at \$22,000. ADIC, 11431 Willows Rd. NE, Redmond, WA 98052, (800) 336-1233, www.adic.com.

SOFTWARE

GFI's MailSecurity Scans E-Mail with Multiple Virus Engines

MailSecurity, from GFI Software, provides gateway-level protection for e-mail against viruses and malicious HTML scripts. It also performs content scanning for inappropriate or proprietary content in outgoing e-mails.

The software combines multiple virus scanning engines to ensure virus detection and decrease reliance on a single vendor's updates. The engines include Norman Virus Control and Softwin's BitDefender. The McAfee anti-virus engine is also available for an additional fee. MailSecurity also detects HTML scripts embedded in e-mail. HTML code is scanned and cleaned before being passed to end users.

Besides virus scanning, MailSecurity also checks both inbound and outbound e-mail for administrator-defined keywords, phrases, and unwanted attachments such as MP3 files. The software searches both subject lines and body text for keywords that might indicate inappropriate language or proprietary information that shouldn't be allowed to leave the organization. Administrators can apply these screening methods globally, or to individual users. E-mail that violates the screening policies can be quarantined for later examination.

MailSecurity is available as an API for Exchange 2000 or for a standard SMTP gateway server. Pricing starts at \$295 for 10 users. GFI Software, 105 Towerview Ct., Cary, NC 27513, (919) 388-3373, www.gfi.com.

Resurrect Old Laptops as Wireless VPN Gateways

Sputnik's Enterprise Gateway software can turn an Intel-based PC into an IEEE 802.11b (Wi-Fi) or 802.11a (Wi-Fi5) wireless access point, complete with router, firewall, and VPN gateway. It's expandable through plug-ins, which allow it to work with popular directories, network management frameworks, and security systems. Included plug-ins support Lightweight Directory Access Protocol (LDAP), Novell NDS, Microsoft Active Directory, CA Unicenter, IBM Tivoli, HP OpenView, Remote Authentication Dial-In User Service (RADIUS), biometrics, and smart cards.

The software is fully open-source, so new plug-ins can easily be developed by third parties. It includes its own version of the Linux OS, and therefore requires a dedicated PC, which must have a 486 or better processor, a bootable CD drive, at least 32Mbytes of RAM, an Ethernet port, and an 802.11 card based on Intersil's chip set. It's available for free download from Sputnik's Web site, or on CD for \$10.

The Enterprise Gateway can optionally be made into a node on Sputnik's own wireless network, meaning that it sells your excess bandwidth to customers within range. (Your own traffic will get priority, thanks to its QoS schemes.) In return, your users can gain free access to other nodes, or you can receive a portion of Sputnik's revenue.

Sputnik, 6034 Fulton St., San Francisco, CA 94121, (415) 354-3342, www.sputnik.com.

SERVICES

AT&T Enhances VoIP Suite

AT&T has enhanced its managed Voice over IP (VoIP) suite, adding greater access, lower pricing, and improved management capabilities. Customers can obtain full connectivity for VoIP/FOIP (Fax over IP) from any VoIP-enabled site, regardless of access technology (IP, ATM, or frame relay). On-network calls (when both parties are AT&T VoIP-enabled) benefit from typical low-cost IP pricing; if a VoIP site calls off-network, the service allows VoIP calls to "hop off" to the global PSTN at off-network rates that undercut circuit-switched pricing.

With global reach into over 50 countries, AT&T is targeting large and medium-sized businesses with international presence that want a managed, lower-price alternative to the PSTN, at speeds up to T3. The service suite is comprised of AT&T Managed Internet Service (MIS) with VoIP, Managed Data Network Service with VoIP, and Managed Router Service with VoIP.

Suite upgrades are currently available. Pricing is set on an individual customer basis. AT&T, 55 Corporate Dr., Bridgewater, NJ 08807-1265, (800) ATT-3199, www.att.com.

Short Takes

HARDWARE

MTI's new Vivant 400 is a 2Gbit/sec Fibre Channel array with a performance level of more than 350Mbytes/sec. The system is available in both Storage Area Network (SAN) and direct-attached models, and is available in rack-mount, 20- and 70-inch cabinet, and tower configurations. The Vivant 400 supports MTI Data-Sentry local and remote mirroring software, and can perform multi-site replication and point-in-time data snapshots. The average price for a multi-Terabyte system is \$200,000.

SOFTWARE

Computer Associates's Unicenter ServicePlus service level management software consists of five tools that can be purchased in an integrated platform or on a stand-alone basis. These tools include a Web- and wireless-based service desk platform for automated workflow and support management, a customer service module, and collaboration tools. ServicePlus also includes predictive tools with notification capabilities as well as knowledge management tools. Pricing starts at \$3,000 per concurrent user.

SERVICE

Gemplex has released a suite of five global IP VPN services running across the Internet and the company's private Multiprotocol Label Switching (MPLS) network. Private IP and Private IP Plus are MPLS-based VPN services. Private IP provides access via partner networks across 37 countries while Private IP Plus provides access directly through a Gemplex node. Flexible IP and Flexible IP Plus are IPsec-based VPNs running across the Internet. Flexible IP Plus drops the traffic off at the nearest Gemplex POP for transport across its MPLS backbone. Mobile IP VPN enables users to access the Gemplex network through IPsec tunnels across the Internet. *

The most critical component of the network doesn't have a MIB... yet.

Monitoring the End User

by Lenny Liebmann

In the early days of IT, network management was "atomic." The objective was to maintain the health of each hardware and software component in the network. The chain was as strong as its weakest link. Find the weakest link and system performance was ensured. In distributed—and later Web—environments, interdependencies between components became more complex. A little latency here, an inefficient database call there, and things could fall apart without any individual component in a critical state. Such negative synergies gave rise to end-to-end response time monitoring—something we're getting pretty good at now.

The next stage in the evolution of network management is likely to center even more on the end user. Monitoring the end user's application "experience" is only the beginning. Today, we're also monitoring the Web sites that end users visit, as well as the volume of network resources they consume. We log their phone usage and detect whether or not they've tried to access confidential data. In fact, there's very little about the end user that we can't find out if we want to.

While some might find such management activities distasteful, these doings are actually a direct consequence of technology having so fully empowered the knowledge worker. In the days of the data center, users couldn't really do anything meaningful, so their behaviors were irrelevant. Now users can do all kinds of stuff. They can create and access extremely valuable information. They can make smarter decisions. They can expedite business processes and make customers happy. By the same token, they can jeopardize security, open up the company to lawsuits, and vaporize irreplaceable data. With power comes accountability—and thus the need to better manage end users. Such management activities are therefore a sign of workplace liberation, not corporate fascism.

HUMAN FACTORS

In light of this growing focus on users, network managers should be aware of a few

things. First, the monitoring of user behavior doesn't violate anyone's constitutional rights. Court cases such as O'Connor vs. Ortega have upheld the employer's right to ensure the proper usage of its tools. To eliminate any expectation of privacy, however, employers must properly notify users that they're being monitored. IT should also consult with corporate counsel to verify the kosherness of the measures that it takes to monitor user behavior.

Second, just because network managers are in charge of deploying the technologies required to adequately monitor user behavior, that doesn't mean they should get involved in enforcement and policy. That's a matter for human resources, legal, finance, and business line management. One way to get as far out of the loop as possible is to use a Management Service Provider (MSP)- or Application Service Provider (ASP)-type resource to gather relevant data and provide reports to the appropriate departmental staff.

Third, make sure that any data you're asked to develop is backed by a clear policy of action. Users aren't servers—you can't click on an icon to reboot them. If they're doing something wrong, their behavior can only be modified through tangible consequences. These consequences are up to human resources to formulate, but you do have a right to ask what the consequences are, so that you don't waste your time gathering data for a policy that's ultimately not going to be enforced.

By the same token, users should be rewarded or commended for exceptional conduct. An end user who alerts the help desk about a questionable e-mail, for example, deserves recognition. After all, people are the most important line of defense against malicious code.

LOOKING AHEAD

In my opinion, we're just starting to understand the value of monitoring users. We have some fragmented data on them—how many calls they've made to the help desk, what kind of long distance charges they run up, how much time they actually spend using the network every day, whether they telecommute, and so on—but we haven't created a truly integrated view of the user in the same way

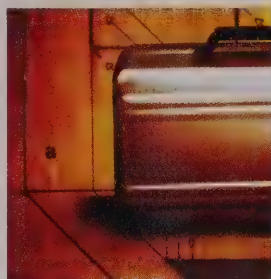
that we've created an integrated view of our infrastructure. As a result, we can only speak in the most general terms about what it costs to support them. We don't know whether there are users who cost 25 times more to support than the average user, or whether those more expensive users are in fact more productive. We therefore have no way of figuring out what it takes to make people more productive or how to lower our support costs.

It's also interesting to note that, while we assiduously track the way customers navigate our Web

sites to make sure that they're as easy to use as possible, we rarely do the same for our intranet Web portals. Management of enterprise users remains reactive rather than proactive. As organizations try to use IT to get leaner and meaner, these inadequacies in our understanding of how people use our costly technology resources will become less tolerable.

So it's time once again to rethink our attitude toward the end user. If we believe that by neglecting to track their behavior, we're somehow showing end users some kind of digital courtesy, we may very well be mistaken. They might be better served if we got to know more about them. *

Lenny Liebmann is a consultant and writer specializing in the business applications of networking technologies. He can be reached at LLmann@comcast.net.

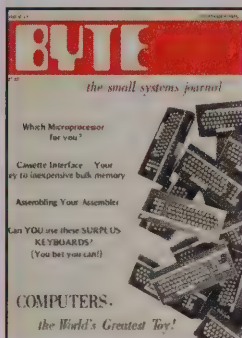
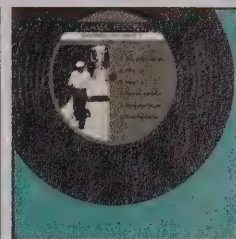
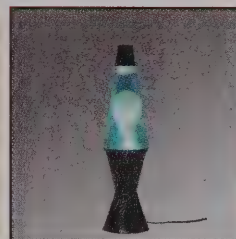


There's very little about the end user that we can't find out.

A special issue of one of the greatest computer magazines EVER is coming soon...

BYTE's Back!

BYTE was born when **bell bottoms**, **lava lamps**, and **vinyl records**, were still groovy.



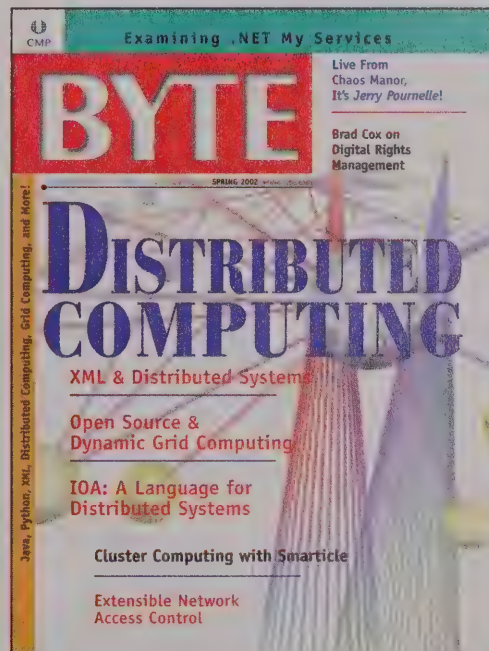
It was the beginning of the personal computer revolution and BYTE was there leading the way with valuable technology information...

In the Spring of 2002, *BYTE* returns with the same kind of in-depth technical analysis of emerging technologies, architectures, and standards shaping the next generation of applications, platforms, and devices.

It features the return of long-time columnists like Jerry Pournelle and Jon Udell. And you'll read about:

- Grid Computing
- Microsoft's .NET My Services technology
- Cluster Computing
- Large-Scale Dissemination of XML Data
- Extensible Network Access Control
- Distributed Digital Rights Management
- And more!

Don't miss out on this special issue of one of the greatest computer magazines EVER!



Look for it on your newsstand or visit
www.byte.com/sub/
to buy your personal copy.*



US Telephone: 1-800-444-4881
International Telephone: 1-785-841-1631
Fax: 1-785-841-2624
Email: orders@cmp.com



VPNs might be tunneling more through your firewall than you'd like.

VPN Vulnerabilities

by Rik Farrow

Your organization probably uses one or more firewalls to control access to your internal networks. You might also use Intrusion Detection Systems (IDSs) to monitor internal systems. Your company certainly uses anti-virus software to detect and remove the malware commonly plaguing Microsoft systems. And, to provide safe remote access, your organization might use IPSec VPN client software so remote users can securely link to your internal networks.

These VPN tunnels can carry much more traffic than you expect. Most remote VPN client software only directs IP traffic destined for your internal network through the VPN tunnel. All Internet traffic is routed directly to the Internet, leaving the VPN tunnel vulnerable to an attacker hoping to use the remote client to relay attacks through the VPN tunnel.

Farfetched? Not really, as the most popular Trojan Horses for Windows include the relay software necessary to accomplish this—software that can pass an attack from the Internet through your firewall using the VPN tunnel. Trojan Horses can wind up on Windows desktops in many ways, most commonly through the spread of viruses that exploit Microsoft software. Securing your network means securing every remote system that connects via VPN.

ILLUSION OF SAFETY

VPNs provide an illusion of safety. Just as Secure Sockets Layer (SSL) encrypts data sent from a browser to a Web server, but doesn't protect the Web server from attacks, a VPN doesn't protect the internal network either. VPNs provide confidentiality of transmitted data, but that data might include passwords that attackers can use against someone's internal network—if the attackers can get inside. And the VPN can serve as the path through the firewall.

In the summer of 2000, an attacker embarrassed Microsoft by using Point-to-Point Tunneling Protocol (PPTP) to gain entry into part of its Redmond campus network. The attacker had installed a Trojan Horse that captured keystrokes and

sent those keystrokes to an e-mail address in Russia. The captured keystrokes included the username and password necessary to use PPTP, and the username and password needed to authenticate to the Microsoft internal domain account. The attacker spent an undetermined amount of time within Microsoft until an astute system administrator noticed that a new user account had been created, most likely as a side effect of an elevation of privilege attack.

Other VPN products don't rely on domain authentication. Most VPN products, including popular remote client software in use today, implement IPSec. IPSec provides standard methods for setting up security associations (paired tunnel endpoints), key exchange, message integrity, and encryption (encapsulation) of messages. Most versions of IPSec interoperate today, if you can match the Internet Key Exchange (IKE) and IPSec Security Association (SA) parameters (see Resources on page 84).

You can also use SSL and Transport Layer Security (TLS) to encrypt traffic. Netscape designed SSL as a method for encrypting communication between browsers and Web servers. TLS is the Internet standard that evolved from SSL. Both rely on digital certificates for authentication, but typically, only the server has a certificate and gets authenticated.

More technical users often employ Secure Shell (SSH), which provides command line access and can also tunnel other protocols. However, you can't use SSH the same way you use a VPN tunnel, as each protocol requires its own tunnel, except for X Window. Most remote users run versions of Windows and use VPN clients with IPSec.

After a remote VPN client is configured, usually when the IT department adds a

new user to the firewall or VPN endpoint, the remote user just needs to connect to the Internet. Then, if all goes well, as soon as the user attempts to access the internal network, a VPN tunnel into the internal network is set up automatically. The user can now access the internal network, knowing that all traffic between the remote system and the internal network is encrypted.



VPN client software doesn't control what enters the internal network.

RELAY REALITY

VPN client software doesn't control what traffic passes into the internal network. And, in most configurations, neither does the VPN endpoint, which might be a firewall, a special VPN appliance, or a software-based VPN server. The VPN endpoint might sit in the firewall, next to the firewall (the Cisco solution), within the internal network, or in front of the firewall (outside or inside a Demilitarized Zone [DMZ]). Except for the last configuration, outside the firewall, anything an attacker can relay through a remote system shows up on

the internal network. Commonly, an attacker's address appears as part of the internal network, depending on how you configure the VPN client.

You can configure your firewall, if it's your VPN endpoint, to permit only certain traffic through the VPN tunnel. After all, the VPN tunnel makes a remote system, one over which you have little control, part of your internal network. But what happens if the laptop with the VPN client on it is stolen? You'd better make sure that tunnel setup requires at least a password, which isn't saved on the laptop itself. If not, anyone who acquires the laptop can access the internal network. Likewise, an unprotected file share can expose the client configuration and stored certificates, allowing someone else to copy the VPN client configuration.

They say "What you don't know can't hurt you."

They're wrong!

Especially when it comes to the security of your network. It's not enough to know who's there; you need to know what they're doing and whether it's acceptable behavior.

NFR Security is the leader in network intrusion detection with a reputation for providing the most powerful and thorough monitoring facilities for detecting attacks and abnormal activity. Combine this with installation and management capabilities that are deceptively simple to use, a flexibility that allows you to customize as much or as little as you want and a tamper-proof system; and you will understand why so many organizations rely on us to protect their networks.



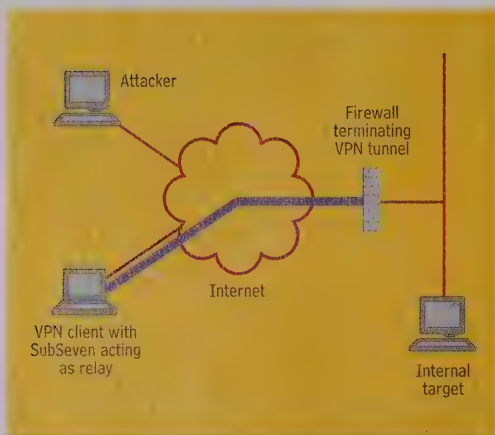
For further information or to request free evaluation software, contact us.
E-mail: sales@nfr.com
Phone: +1 240 632 9000 Fax: +1 240 632 0200
www.nfr.com

Resources

For information on CORE Competence VPN and FAQs, go to www.corecom.com/external/vpn/vpnfaq.htm.

To access the IPSec IETF Charter page, with links to standards (RFCs) and draft standards, click on www.ietf.org/html.charters/ipsec-charter.html.

Information on the capabilities of SubSeven, including relaying, is available at <http://rr.sans.org/malicious/subseven2.php>.



Getting a Free Ride Past the Firewall. The attacker uses relay software installed on the notebook to enter the VPN tunnel, eventually attacking the system labeled "internal target."

The relay software comes courtesy of Trojan Horses like SubSeven (see Resources), which include the ability to remotely scan and to relay connections. The attacker can configure the Trojan Horse so it can relay traffic through the remote system into your internal network. The relayed traffic has the same source address as the remote system and uses the same VPN tunnel. For the attacker, life is good. For the defender, the firewall and VPN don't work as expected (see figure above).

You can employ software today that provides at least part of the answer to this security problem. You need to treat remote systems like local systems—they must be protected by firewall software and the latest anti-virus software and signatures. The firewall software can be a personal firewall. Some vendors, such as SafeNet (www.safenet-inc.com), include a personal firewall as part of their remote

VPN client. If the personal firewall prevents access to any relay part of a Trojan Horse, you've partially solved this problem. Of course, if the Trojan Horse designer has found a way to bypass the personal firewall, such as using what appears to be Web traffic coming from `iexplorer.exe`, then the firewall might not be enough.

You must have the other piece of the solution: anti-virus software. Anti-virus software has been able to detect known Trojan Horses for a long time. Your policy must dictate that remote users employ the latest anti-virus software and get routine updates, to avoid infection by a tricky Trojan Horse. The policy must also require properly configured firewall software.

Your organization could also take another step, although it might not be simple. The remote system could route all traffic, even Internet-directed traffic, through the VPN tunnel. Once within the internal network, the Internet-directed traffic would have to pass through your corporate firewall, which could enforce whatever policies you want on that traffic. A side effect of this would be to block most relays.

Another side effect is the increased latency involved in having Internet traffic pass through the firewall not once, but four times: in via the VPN, out to the Internet, the reply back in through the firewall, then out via the VPN to the remote client. Even popular VPN software today doesn't make this easy. You can do it manually by installing a default route through the VPN tunnel.

POLICY POLICING

Having a policy that requires remote users, whether they're working at home or on the road, to use properly configured and updated firewall and anti-virus software is important. Enforcing this policy is a fantasy.

If everyone who works in your organization has the utmost regard for security and rigorously follows your policy, you won't have problems with your remote systems. Experience shows that most people generally disregard security, with high-level executives the worst offenders. It would be nice if a software mechanism could enforce policy, but this isn't currently possible.

Software that can enforce policy is software that could be replaced or subverted. Even OSS aren't immune to corruption, because kernel modules that subvert both Unix and Windows server

OSs exist and can bypass any security regimen. Software that can provide updates of anti-virus signatures each time a remote user opens a VPN tunnel into the home office help. There's a danger that if the update software can be subverted, the security system becomes as dangerous as SubSeven. Still, a product that can remotely enforce security policies would be a better solution than what we have now.

VPNs that connect branch offices face similar issues. Does each branch office follow the same security policy? Does the branch office even have a firewall? Have they recently updated their anti-virus software? These are the same issues that face organizations that use T1s, ATM, or frame relay virtual circuits to connect remote sites together. Each site must have the same security policy and maintain that security policy at the same level.

For example, imagine that your organization has offices in another country and that you have a VPN tunnel between the remote office and your local office. You already know how difficult it is to get your fellow workers to follow good security practices. How are things going in the overseas office? You don't want to find out the hard way, by means of an attack or virus infection that comes through the VPN.

You can also imagine attempting to achieve good security practices in an e-business environment, where you permit approved business partners access to certain services within your internal network. The problem is, you have no control over your partner's security policy and practices.

The most important things to remember about VPNs are simple. VPNs protect against eavesdropping and insertion attacks. A VPN doesn't stop an attack from being passed through it. You can, of course, terminate the VPN tunnel outside your firewall, on a DMZ subnet, and some organizations do this—but not many. You can also apply firewall rules to VPN tunnels that terminate at a firewall. But again, most companies don't do this. As noted in another "Network Defense" column ("Secure Sockets Layer Is Not A Magic Bullet," January 2001, page 108), encryption isn't a cure-all, but just another tool you must use correctly to achieve the results you want. *

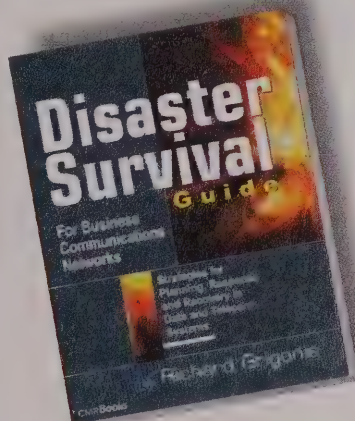
Rik Farrow is an independent security consultant. His Web site, www.spirit.com, contains security links and information about network and computer security courses. He can be reached at rik@spirit.com.

CMPBooks

Disaster Survival Guide for Business Communications Networks

Protect your business from natural and manmade disasters. This book explores strategies and solutions for disaster planning, mitigation, response and recovery for data and telecom systems and networks. Discover which technologies keep your business running and protect your employees from unnecessary risk.

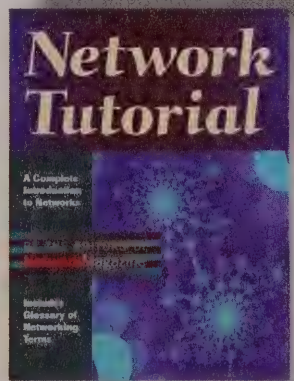
ISBN 1-57820-117-9, \$49.95



Network Tutorial

Explore the networking industry – from the basic concepts of networks through protocols, hardware and software components, and the unique jargon of networking – with this easy-to-understand guide. The extensive glossary provides a quick reference for unfamiliar terms.

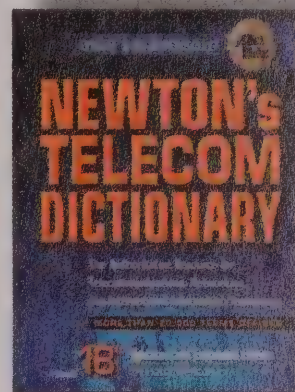
ISBN 1-57820-044-X, \$29.95



Newton's Telecom Dictionary, 18th Edition

Keep up with the ever-changing telecom and Internet markets with this industry "bible". With over 20,000 definitions – including intranet, broadband services, wireless and e-commerce terms – this edition is over four times larger than its nearest competitor. Harry Newton uses non-technical language to explain these technical concepts.

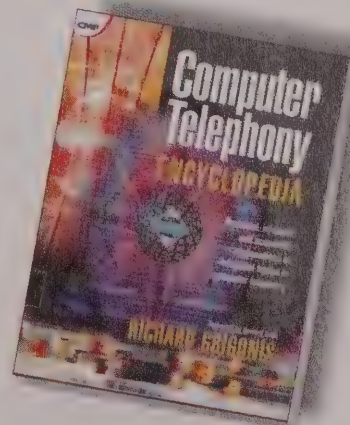
ISBN 1-57820-104-7, \$34.95



Computer Telephony Encyclopedia

Get up-to-speed on hundreds of computer telephony topics with thorough, practical and straightforward explanations that include usage, how the subject relates to other technologies and a buyers-guide-like discussion of products based upon current technology.

ISBN 1-57820-045-8, \$39.95



Find CMP books
in your local bookstore

800-500-6875
cmp@rushorder.com

Optimists may have more fun, but pessimists are usually right.

How Vendors Use Math to Lie

by Andy Dornan

It's been thirty years since the Club of Rome, a then-influential think tank of scientists and economists, published the worldwide best-seller *The Limits to Growth*. Its message was simple: Exponential growth cannot continue indefinitely. Instead, the authors predicted, finite supplies of natural resources will eventually lead to catastrophic shortages of food, water, and energy sources.

Though resonant at the time, its warnings have now become an example of unwarranted scaremongering, on the basis that doomsday did not occur. But, in fact, the Club's timescale was a full century (not a mere thirty years) and its shorter-term forecasts have proved accurate. Perhaps of more immediate concern, people have forgotten its most basic point—that in the real world, exponential growth does run up against physical limits.

Networking industry analysts could benefit from this insight. Many of their predictions about the impact of a technology or product seem to be based on extrapolating current or past trends, without considering any limit. It should be obvious that no company can achieve more than 100 percent market share, and that customers will buy fewer cell phones once everybody already has one.

The greatest exaggerations come from vendors, of course. Nokia has long maintained that there is no real limit to the cell phone market, that people will gladly own several each. NTT DoCoMo goes further, estimating that by 2010, each person in Japan will buy a new mobile data device approximately every 80 days. So far, the evidence is against both: DoCoMo is

already having trouble convincing its i-mode data users to upgrade to third-generation (3G), let alone use two phones. And while wireless data may eventually be built into many types of electrical appliance, this is more likely to be in the form of a short-range LAN or cable-replacement technology than a public network service involving a cellular operator.

The limits imposed by the laws of physics have a particular impact on wireless networking: While you can always lay new cables, there's only one radio spectrum, and its information capacity is fixed. As a result, vendors wanting to deliver exponential increases in bandwidth must resort to ever-greater hype.

The only way to distinguish between hyped data rates and real throughput is thorough testing. However, the equation below should provide a rough guide. If you're not fluent in algebra, don't worry. It's all division and subtraction, though the number of minus and fraction signs is increasing all the time.

LIMIT SUMS

The most recent "innovation" in hype is to add together the data rates of all channels used by a radio system, giving a theoretical total capacity of the airwaves. This is equivalent to calculating an Ethernet network's capacity by adding together the speed of each port on every switch within a 100 meter radius—even those located in someone else's building. The first step in finding the real throughput is to divide the hyped capacity by the number of channels used.

Fortunately, this number is still one in most cases, but there are exceptions. Proponents of IEEE 802.11a, for example, claim that it provides over 1Gbit/sec in Europe. Though 802.11a is possibly the best wireless technology yet shipped, it isn't that good. The figure assumes 19 separate networks of 54Mbit/sec each.

Still sounds fast, but no application will ever see that speed. Protocol overhead

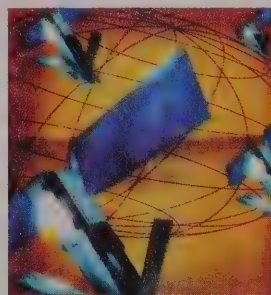
eats up a significant proportion of bandwidth in wireless networks, thanks to signaling and forward error correction. While regular Ethernet's overhead can often be ignored, that of its wireless equivalent consumes nearly half of the available bits. Once the data link layer headers are stripped off, 802.11a's 11P throughput is a more modest 31Mbit/sec.

The next step is to factor out compression and factor in interference. Existing cell phones generally do this, really delivering on their modest promise of 9.6Kbit/sec, but many 3G systems don't. The upgrades planned by U.S. operators will be particularly susceptible to this, as they rely on new modulation that requires a clear signal.

Other 3G systems, such as those in Japan and Europe, are more affected by the number of users contending for a radio channel. The hyped speeds of 2Mbit/sec or more usually assume a single user, next to a base station. In real systems, the available bandwidth is shared. Packet switching helps to share it more efficiently for data applications, but telephony and streaming media still require a fairly constant bit rate.

The final issue to consider is duplexing, which can reduce throughput by a factor of two. Most 3G networks already take this into account, because they're asymmetric and quote separate speeds for the upstream and downstream link, but wireless LANs don't. Even under ideal interference conditions, the maximum two-way throughput of an 802.11a link is about 15Mbit/sec. That's still more than enough for most applications, but it's a long way from the "gigabit" claims. The gap between hype and reality is one area where growth seems truly unlimited. *

Senior editor Andy Dornan's newly revised book, *The Essential Guide to Wireless Communications Applications*, ISBN 013-0097-187, is out now. He can be reached at adornan@cmp.com.



$$R_L = \frac{H}{\lambda} - \sum_{i=1}^{L-1} P_i$$

$$\Omega \times c \times d \times n$$

Calculating the Truth. R_L = Real throughput at layer L; H = Hyped data rate; λ = Number of radio channels; P_L = Layer L protocol overhead; Ω = Interference; d = duplex factor; c = compression; n = number of users.



Advertiser Information

American Power Conversion	17	Qualcomm	29
Array Networks	S9	Radware	C3
Artiza Networks	27	SAP	C4
Avocent Corporation	25	SonicWALL	S3
Computer Associates	31	Sophos	13
Cyberguard	S7	Sourcefire	S5
F5 Networks	9	Sprint North Supply (North America ONLY)	43
Finisar	23	Trend Micro	C2-1
Fluke Networks	6		
Hewlett Packard	19		
Hoffman	39		
IBM DB2	2-3		
IBM Tivoli	4-5		
NECA	21		
Net To Net	55		
Network Instruments	94		
NFR Security	83		
Novell	11		
Panduit	15		

The advertisers' index is provided as a service to readers.
The publisher assumes no liability for errors or omissions.

NORTHWEST / SILICON VALLEY

Jenny Gutierrez
(415) 947-6358 / F (415) 647-6022
jgutierrez@cmp.com

SOUTHWEST / MIDWEST 1*/ WESTERN CANADA

Jenny Gutierrez
(415) 947-6358 / F (415) 647-6022
jgutierrez@cmp.com

ASSOCIATE PUBLISHER / NORTHEAST EASTERN CANADA

Amy Ventura
(212) 600-3084 / F (212) 600-3175
aventura@cmp.com

SOUTHEAST / MIDWEST 2**

Cara Capasso
(212) 600-3024 / F (212) 600-3175
ccapasso@cmp.com

EUROPE

Michael Taylor
+44 1244 315695 / F +44 1244 315695
mikestay@aol.com

MIDDLE EAST / ITALY

Rhonda T. Abramson
M@RS Marketing
+972-9-891-0611 / F +972-9-891-0644
rhonda@actcom.co.il

NATIONAL SALES MANAGER, DIRECT RESPONSE

Bethany Baller
(585) 342-2484 / F (585) 342-2488
bballer@cmp.com

ASSOCIATE PUBLISHER / MARKETING DIRECTOR

Amy Gamba Rouas
(415) 947-6354 / F (415) 947-6022
arouas@cmp.com

MARKETING COORDINATOR

Ann Freccero
(415) 947-6734 / F (415) 947-6022
afreccero@cmp.com

PUBLISHER

Karla Johnson
(212) 600-3067 / F (212) 600-3175
kjohnson@cmp.com



NetworkMagazine MARKETPLACE

SALES TERRITORIES

NATIONAL MARKETPLACE

NATIONAL SALES MANAGER,
DIRECT RESPONSE

Bethany Baller

phone: 585.342.2484

fax: 585.342.2488

bballer@cmp.com

HARDWARE

		PAGE
ABA Industry	www.aba-industry.com	103
buyuptime.com	www.buyuptime.com	98
Cyclades	www.cyclades.com	90
GL Communications	www.gl.com	102
Global Technology Associates	www.gta.com	95
L-com	www.l-com.com	100
MovinCool	www.movincool.com	91
Digital Warehouse	www.digitalwarehouse.com	102
Network Hardware Resale	www.networkhardware.com	100
Network Technologies	www.nti1.com	102
Omnitron Systems Technology	www.omnitron-systems.com	93
Raritan Computer	www.raritan.com	89
Rose Electronics	www.rosel.com	99
Server Technology	www.servertech.com	96
Spectrum Control	www.spectrumcontrol.com	92
Western Telematic	www.wti.com	96

SOFTWARE

Blue Ocean Software	www.blueocean.com/demo/nma.htm	102
Network Instruments	www.networkinstruments.com	94

TRAINING / CERTIFICATION

LearnKey	www.learnkey.com	103
Self Test Software	www.selftestsoftware.com/sho/network/	94

FURNITURE / RACKS / ENCLOSURES

American Power Conversion - APC	www.apc.com	101
Anthro	www.anthro.com	90
Ergotron	www.ergotron.com	97
Global Computer Supplies	www.globalcomputer.com	92

2002

KVM Access Over Web Browser™

2001

KVM Access over IP

If having remote access to your servers over IP means installing proprietary software or PCI cards, that's not convenient, anywhere, anytime access. Introducing the new, multi-port TeleReach®.

1999

KVM Access over Cat5

TeleReach is the easiest, most secure way for one or more users to remotely access and manage multiple servers through a KVM switch, from any PC running the Internet Explorer® 4.0 browser.

To see and feel the power of remote KVM access over Web browser, **call Raritan Sales at (800) 724-8090** to sign up for a live demo from your own desktop.

Intelligent KVM Switch Technology

 **Raritan.**
www.raritan.com

800-724-8090
732-764-8886

1988

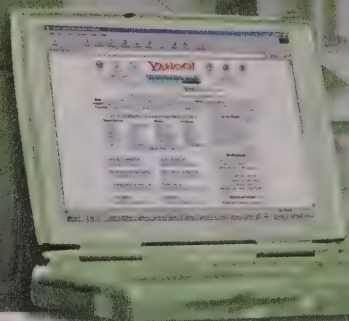
KVM Access over Coax



FURNITURE
RACKS
ENCLOSURES

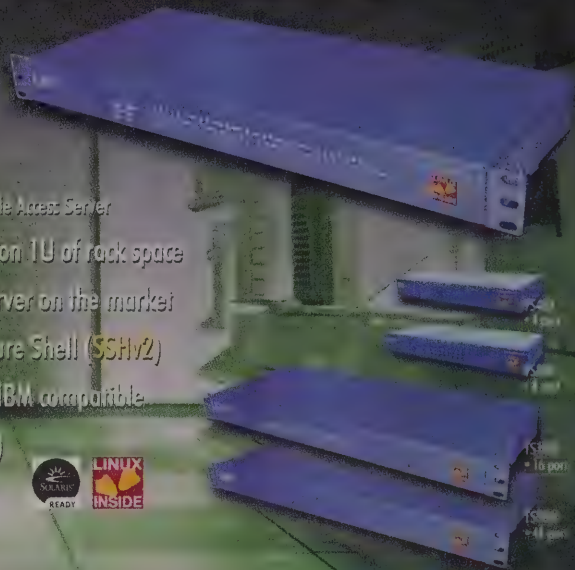
Guess what Yahoo! uses to manage their servers?

"The Cyclades-TS Series of Console Access Servers provides the highest port density and security at a very competitive price. By using Linux as the embedded OS, it offers the flexibility required to manage our dynamic environment. The Cyclades-TS is a key element to help us keep our servers up and running." - Pete Kunitz, Manager of Site Operations, Yahoo! Inc.



Cyclades-TS Series Console Access Server

- 1/4/8/16/32/48 RS-232 ports on 1U of rack space
- First Linux-based Terminal Server on the market
- IP Filtering, RADIUS, and Secure Shell (SSHv2)
- Linux, FreeBSD, Sun, HP, and IBM compatible
- No unintentional breaks (Sun)
- Off-line data buffering



Request for your FREE CAS booklet at www.cyclades.com



THE LEADER IN
LINUX
CONNECTIVITY

www.cyclades.com

1-888-CYCLADES 1-888-292-5233
sales@cyclades.com

CYCLADES

©2002 Cyclades Corporation. All rights reserved. All other trademarks and product images are property of their respective owners. Product information subject to change without notice.

Furniture Solutions that Work!

Configure your workstation exactly for your application. With lots of sizes and accessories available, not to mention a Lifetime Warranty, you get ultimate flexibility and incredible strength. Give us a call or visit our web site to see all the possibilities!



ANTHRO

800.325.3841
anthro.com



Over 10,000 Companies Spot Cool With MovinCool.



Shouldn't You Put Us On The Spot Too?



MovinCool has been #1 in portable spot cooling for over 20 years. In fact, recent independent tests show that MovinCool outperforms the nearest competitor in cooling capacity (BTU/h), energy efficiency (EER) and airflow (CFM). No wonder we're the #1 choice of over 10,000 companies! Shouldn't you put us on the spot too?

- Protects against excessive heat
- Prevents costly system failures
- Programmable temperature controls
- Up to 60,000 BTU/h of cool air
- No costly installation
- Affordable emergency back-up

MOVINCOOL®

THE #1 PORTABLE SPOT COOLING SOLUTION

Call 800.264.9573 or visit www.movincool.com

Your network costs a fortune... ...protecting it doesn't have to.

**NEW
LOWER
PRICES!**



72" Workstation
\$799
Stk. # C95033

Keyboard drawers and casters sold separately.

GLOBAL
COMPUTER Systemax

www.globalcomputer.com/go/mag/lan

Global LAN Furniture protects your equipment for a lot less money.

Our heavy-duty LAN Furniture is built to last with steel-reinforced, triple-leg support and lateral braces. Built-in cable management system hides unsightly wires and organizes and separates cables. Deep 30" work surface, adjustable shelves and sturdy server shelf allow for easy integration of all your network equipment, providing a complete storage solution. Our 96", 72", 48" and 24" wide units combine with additional shelves, keyboard drawers and casters for unmatched flexibility to meet your changing needs.

24" Workstation
\$299
Stk. # C20803



**SAVE A TON OF MONEY
ON YOUR NEXT
MEDIA PURCHASE!**
Check out our prices today!

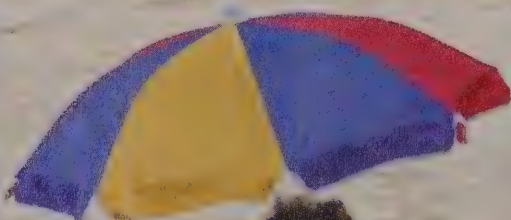


DLT IV
as low as
\$4799

CALL 1-800-8-GLOBAL

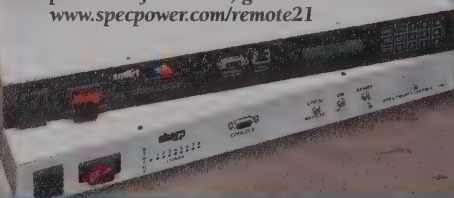
or visit us online for the LAN solution that is right for you.

Ref #NM6/02



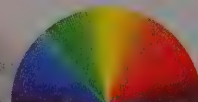
POWER
Technologies Group

To learn more call 814-835-1650
or for Remote Management online
product information, go to
www.specpower.com/remot21



Remote Network Management can be a day at the beach

- Reboot via Built-in modem, LAN/WAN and wireless connections
- Lower costs through reduced network downtime and field service visits
- SMARTstart and SHARPstart PDU's offer customization and are upgradable
- Menu-driven user friendly interface and secure password protection
- Global access to monitor, program, reboot and sequence outlets



SPECTRUM CONTROL INC.
Power Technologies Group
www.specpower.com/remot21

Fiber Media Converters

The Nuts and Bolts of Networking



For Metropolitan Area Networks (MAN) or Local Area Networks (LAN), fiber media converters provide the nuts and bolts that support fiber network connectivity.

Omnitron's managed *iConverter™* with its SNMP *NetOutlook™* management software and the unmanaged *FlexPoint™* converters provide copper to fiber and multimode to single-mode conversions that scale, as the network's needs change.



Ideal for MAN and large LAN applications, the *iConverter™* SNMP managed converters use hot-swappable plug-in modules with a variety of chassis options and AC/DC triple-power-redundancy. The *iConverter™* features advanced fault-detection and trap notification (see table).

The *NetOutlook™* SNMP network management software can monitor, configure and respond to trap notifications from *iConverter™* modules. It runs under Windows™ 9X/NT/2K or under SNMP management systems like HP OpenView™.



Ideal for unmanaged MAN and LAN applications the *FlexPoint™* converters use hot-swappable self-contained modules with a variety of chassis and mounting options and AC/DC dual-power-redundancy (see table).

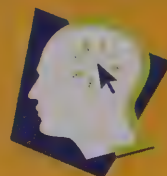
	Managed <i>iConverter™</i>	Unmanaged <i>FlexPoint™</i>
Network Management		
SNMP Based	Yes	-
Telnet	Yes	-
In-Band	Yes	-
Out-of-Band	Yes	-
Traps Supported	Yes	-
Chassis Stacking	16	-
Chassis and Power		
Chassis Types (Size)	19-Unit, 2U 2-Unit, 1U 1-Unit, >1U	14-Unit, 2U 5-Unit, 1U 1-Unit, >1U
Power Source	AC or DC	AC or DC
Power Redundancy	Triple	Dual
Module Types		
10 Ethernet	Yes	Yes
100 Ethernet	Yes	Yes
10/100 Ethernet	Yes	Yes
Gig Ethernet	Yes	Yes
T1, E1	Yes	Yes
RS232	-	Yes
Multimode/Single-mode	Yes	Yes
Special Features		
Fiber/Module Redundancy	Yes	-
Remote Fault Detection	Yes	-
Link Segmentation	Yes	Yes
Link Propagation	Yes	-
Warranty / Service		
Warranty	Lifetime	Lifetime
Technical Support	24x7	24x7
Technical Support Cost	Free	Free

For product information, contact an Omnitron product specialist at:
Omnitron Systems Technology, Inc., 27 Mauchly, #201, Irvine, CA 92618
Phone: (800) 675-8410 or (949) 250-6510 - Email: info@omnitron-systems.com

www.omnitron-systems.com/nm

OST Omnitron Systems Technology, Inc.
The Nuts & Bolts of Fiber Networking

© Copyright 2002 Omnitron Systems Technology, Inc. iConverter, NetOutlook, FlexPoint and the OST logo are trademarks of Omnitron Systems Technology, Inc. All other trademarks are the property of their respective owners.



Self Test
SOFTWARE

PASS THE EXAM!

WWW.SELFTESTSOFTWARE.COM
(800) 244-7330

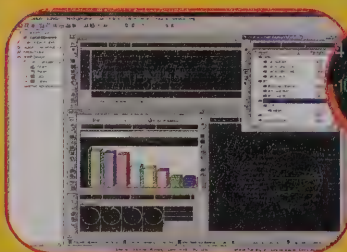
Ten Years of Getting IT Technologists Certified - the First Time!



There Is A Better Way To Troubleshoot & Manage Your Network



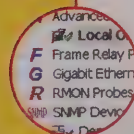
**Quickly Pinpoint,
Pre-solve and Prevent
Network Problems**



Observer
\$995

**Expert
Observer**
\$2895

**Observer
Suite**
\$3995



Observer®—Identifies network trouble spots and costs thousands less than expensive hardware-based analyzers.

- **Full packet capture and decode** for over 500 protocols, including TCP/IP (v4 & v6), NetBIOS/NetBEUI, VoIP, SNA, SQL, IPX/SPX, Appletalk and many, many more!

- **Switched mode sees all ports** on a switch gathering statistics from an entire switch or capture/statistics from any port(s)

- **Long-term network trending** collects statistical data for days, weeks, months, even years

- **Real-time statistics** include Top Talkers, Bandwidth, Protocol Statistics, and Efficiency History

- **Ethernet (10/100/Gigabit), Token Ring, FDDI, and Wireless 802.11**—no need to purchase separate tools

- **Windows® 98/Me/NT/2000/XP compatible**

- **Over 4,000 frame types recognized**

Expert Observer—Includes all of the features of Observer plus real-time and post-capture expert event identification and analysis—new SQL and Frame Relay experts add to the many other protocols covered, time synchronization technology, and modeling of network traffic.

Observer Suite—Provides a full complement of tools that includes all of the features of Expert Observer plus SNMP management, RMON console/Probe and Web reporting. Includes one remote Probe.

If you have any network problems, find out the cause with Observer, Expert Observer, or Observer Suite.

Call 800-526-7919 or visit us online for a full-featured evaluation:

WWW.NETWORKINSTRUMENTS.COM

US (952) 932-9899 • Fax (952) 932-9545 • UK & Europe +44 (0) 1959 569880 • Fax +44 (0) 1959 569881



©2002 Network Instruments, LLC. Observer, "Network Instruments" and the "N with a dot" logo are registered trademarks of Network Instruments, LLC. All other trademarks are property of their respective owners.

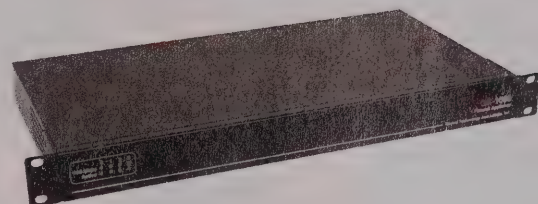
Internet Security

Global Technology Associates

Firewall Appliances

GB-1000 Firewall/VPN Appliance

High performance, firewall with unlimited user licenses, transparent NAT, stateful packet inspection, built-in IPSec VPN, four 10/100 Ethernet interfaces, DHCP server, DNS server, secure remote management and content filtering in a 1RU case. High Availability, gigabyte Ethernet and additional interfaces are optional.



RoBoX Firewall

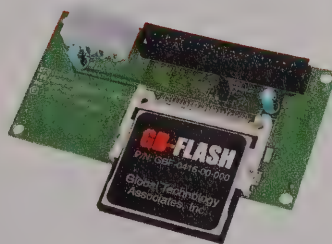
Remote/branch office firewall for up to 25 concurrent outgoing users. Features include transparent NAT, stateful packet inspection, built-in IPSec VPN, content filtering and three 10/100 fully configurable Ethernet connections packed in a 6" square case. Big security for small offices!



Firewall Software Systems

GB-Flash

All the power of the ICSA certified GNAT Box system software on an easy to install, solid-state flash memory module that plugs into the system motherboard. Features include transparent NAT, stateful packet inspection, built-in IPSec VPN, DHCP server, DNS server, secure remote management and content filtering.



GNAT Box Pro

Simple, powerful ICSA certified firewall solution. It runs and boots from a floppy, requiring only a 486 CPU and 16MB memory. Features include built-in IPSec VPN, secure remote management and support for hundreds of network cards including gigabyte Ethernet.



**Global
Technology
Associates, Inc.**



Sales: (800) 775-4GTA
Tel: (407) 380-0220
Email: info@gta.com
Web: <http://www.gta.com>



How do you reboot 16 equipment units...

using Zero U of rack space?



16 remotely addressable power outlets — The highest density available of any Remote Power Management vertical strip. 30-amp power input feed distributed across 16 outlets.



Mounts vertically in your equipment rack or cabinet and requires Zero U of rack space. Load Sense provides real-time current monitoring in the remote screen interface and through a built-in LED display for on-site measurement.

Power-up sequencing of all 16 outlets prevents an in-rush current overload.

Telnet, SNMP, Modem or RS-232 interfaces for easy, practical and secure power management of remote internetworking equipment.



Install the new Sentry Power Tower in your data center, NOC or co-lo facility and gain the advantage of remotely rebooting up to 16 of your equipment units — without occupying any space in your rack or enclosed cabinet.

Try the New Sentry Power Tower in your rack or cabinet and realize the benefits of Intelligent Power Distribution and Remote Power Management.

See our complete product line at www.servertech.com or call 800.835.1515 or 775.284.2000

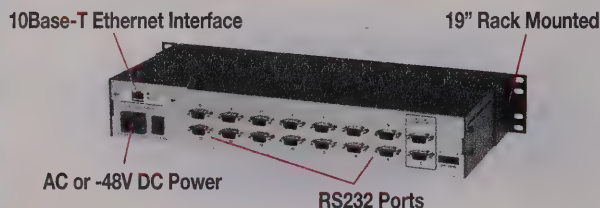
© 2001 Server Technology, Inc. Sentry is a trademark of Server Technology, Inc.

Another great product from
Server Technology, Inc.

Remote Network Management Solutions

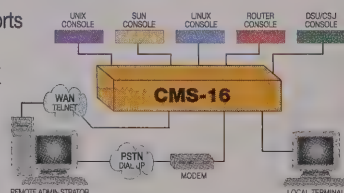
Access Your Network Equipment from Anywhere

Telnet and Dial-Up Console/AUX Port Switch Cost Effective Terminal Server Alternative

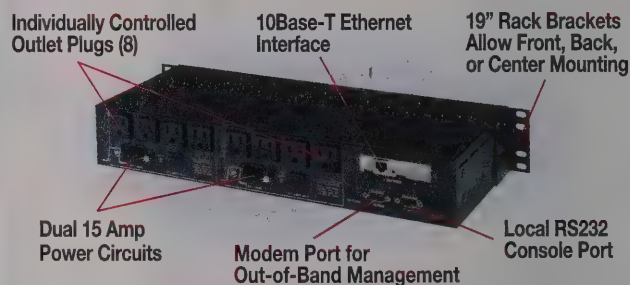


Console Management Switch (CMS)

- 8, 16 or 32 RS232 DB-9 Serial Ports
- Simultaneous Telnet Sessions
- Non-Connect Port Buffering - 32K
- IP Security Features
- Modem Auto-Setup Command Strings (User Definable)
- NEBS 3 Approved



Telnet and Dial-Up Network Power Switch Reboot Locked-up Equipment



Network Power Switch (NPS)

- 8 Individual Outlets
- On/Off/Reboot Switching
- Integral 10Base-T Interface
- Co-Location Features
- Outlet-Specific Password Security
- Network Security Features
- 115-VAC (230-VAC available)
- Power-Up Sequencing



www.wti.com

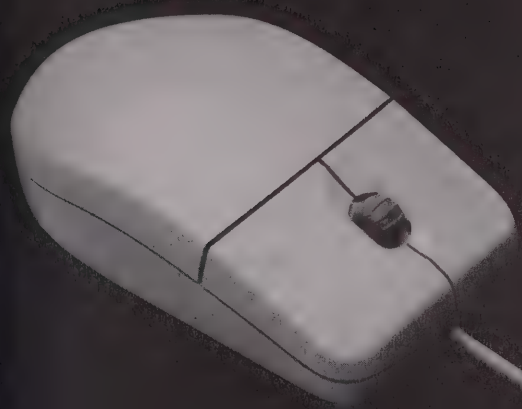
(800) 854-7226

western telematic incorporated
5 Sterling • Irvine • California • 92618-2517

Keeping the Net...Working!

Network Magazine

WHERE THE ENTERPRISE MEETS THE NEW PUBLIC NETWORK



Isn't it time
you got
your own

FREE

Subscription?

Subscribe online today!

<http://subscribe.networkmagazine.com>

or complete the form on the reverse side
and fax to (847) 647-8648



CMP
United Business Media

Network Magazine

WHERE THE ENTERPRISE MEETS THE NEW PUBLIC NETWORK

P.O. Box 2013 • Skokie, IL 60076-7913 • Fax: (847) 647-8648

☐ **YES!** I want to receive/continue to receive **Network Magazine FREE.**

☐ No

Signature

Date

- All questions must be answered to qualify for your **FREE** subscription.
- All forms must be signed and dated.
- Return form by mail or fax to (847) 647-8648. Or, for faster service, subscribe online at <http://subscribe.networkmagazine.com>
- **e-mail address:**

* An e-mail address is **REQUIRED** to contact you regarding your **FREE** Subscription

May we contact you with other offers? ☐ YES ☐ NO

The publisher only accepts applications which meet the qualifications for the publication

<http://subscribe.networkmagazine.com>

FREE Subscription Application

☐ Mr. First Name

Last Name

☐ Ms.

Title

Company Name (Must be supplied)

Division/Mail Stop

Business Street Address (P.O. Boxes not accepted on this line)

City

State

Zip

Country

Telephone

Fax

If your company would prefer delivery to your home or business P.O. Box, please complete the area below. Company name and address are still required to qualify.

Please mail my copy to: ☐ Home address (below) ☐ Business P.O. Box (below) ☐ Business street (above)

Address

City

State

Zip

If you work from home, for a business located elsewhere, please list both that business address and your home address. If your home address is your ONLY business address please check here. ☐

EKB33 Form 33

1 I currently or will specify, recommend, approve, purchase, or influence the purchase of computer services/hardware/software/applications used in a networked environment: (check one)

01 ☐ Yes 02 ☐ No

2 The primary business activity performed at this location is: (check one)

PUBLIC (Telecommunications/Service Provider/Carrier) NETWORK

- 01 ☐ Online/ISP/Web Hosting
02 ☐ Communication Service Provider (including: Interexchange/PTT/Long Distance/Carrier/Bell Operating or Regional Holding Co./Independent Telephone or Holding Co./Satellite/Cellular/Wireless/Mobile Data Services/Public Data Network/VAN/Interconnect/CLEC/ASP)

03 ☐ Broadcasting/CATV/MSO

04 ☐ Utilities

91 ☐ Other Service Provider:

(please specify)

PRIVATE NETWORK

- 05 ☐ Finance/Banking/Accounting
06 ☐ Insurance/Real Estate/Legal
07 ☐ Health/Medical/Pharmaceuticals
08 ☐ Construction/Engineering/Architecture
09 ☐ Media: Entertainment/Broadcast/Advertising/Publishing/Marketing/Printing
10 ☐ Agriculture/Forestry/Mining/Petroleum/Chemicals
11 ☐ Transportation/Shipping
12 ☐ Government/Public Administration/Military
13 ☐ Aerospace
14 ☐ Research and Development
15 ☐ Education/University
16 ☐ Consulting/Systems/Network Integrator
17 ☐ Manufacturing/Design (Computers, Software, Peripherals, Network Products, Communications Equipment)
18 ☐ Manufacturing/Design (Other than Computer/ Communications Equip.)
19 ☐ Value-Added Reseller (VAR)/Distributor
20 ☐ Computer/Data Processing/Computer Communications Services/Sales/Repair/Leasing/Training
21 ☐ All Other Business Services including Retail/Hospitality/Entertainment/Recreation/Non Profit/Trade Association

99 ☐ Other

(please specify)

3 Which is your primary job function? (check one)

Enterprise Networking/IT Management (VP, Director, Chief, Head, Manager, Supervisor, Project/Group Leader)

- 01 ☐ CIO/CTO
02 ☐ VP IS/IT
03 ☐ IS/IT Management
04 ☐ Networking/LAN Management
05 ☐ Data Communications Management
06 ☐ Telecommunications Management
07 ☐ Security Management
08 ☐ Network Engineering Management
09 ☐ Programming/Systems Management
10 ☐ Internet/E-Commerce Management
11 ☐ Consultant/Outsourcing/VAR/Distributor
12 ☐ Network/Systems Integration Mgmt
91 ☐ Other Networking/IT Management

(please specify)

Corporate Management

- 13 ☐ Executive (Chmn, CEO, COO, Pres, Owner)
14 ☐ Financial (CFO, Treasurer, Controller)
92 ☐ Other Corporate/Departmental Mgmt

(please specify)

Other

15 ☐ Technology Staff

99 ☐ Other

(please specify)

4 Number of employees in ENTIRE COMPANY: (check one)

- 01 ☐ 50,000 or More
02 ☐ 20,000-49,999
03 ☐ 10,000-19,999
04 ☐ 5,000-9,999
05 ☐ 1,000-4,999
06 ☐ 500-999
07 ☐ 100-499
08 ☐ less than 100

5 Annual dollar volume of networking equipment and services I specify, recommend or approve for my organization or largest client's organization: (check one).

- 01 ☐ \$150 Million or More
02 ☐ \$100 Million to \$149.9 Million
03 ☐ \$50 Million to \$99.9 Million
04 ☐ \$20 Million to \$49.9 Million
05 ☐ \$10 Million to \$19.9 Million
06 ☐ \$5 Million to \$9.9 Million
07 ☐ \$1 million to \$4.9 Million
08 ☐ \$500,000 TO \$999,999
09 ☐ Under \$500,000

6 Please indicate the products and/or services you help plan, recommend, specify or purchase. (check all that apply)

INTERNETWORKING PRODUCTS/NETWORK INFRASTRUCTURE

- 01 ☐ Routers
02 ☐ Gigabit Ethernet Backbone Switches
03 ☐ Fast Ethernet Workgroup Switches
04 ☐ ATM Switches
05 ☐ NICs/Adapters
06 ☐ Hubs/Concentrators
07 ☐ Premises Wiring/Components
08 ☐ Fiber Cabling/Connectors
09 ☐ UPSs
10 ☐ Network Printers

WAN PRODUCTS AND SERVICES

- 11 ☐ Internet Access Services
12 ☐ Web Hosting Services
13 ☐ Application Services
14 ☐ E-mail Services
15 ☐ Content Management Services
16 ☐ Frame Relay Services
17 ☐ ATM Services
18 ☐ Leased Line Services (T1/T3, E1/E3)
19 ☐ Outsourcing Services
20 ☐ Load Balancing Devices
21 ☐ Bandwidth Managers
22 ☐ xDSL Equipment
23 ☐ Remote Access Hardware/Software
24 ☐ Policy Based Networking Equipment
25 ☐ CSU/DSUs/Multiplexers

NETWORK SOFTWARE

- 26 ☐ Network Management Systems
27 ☐ Directory Services
28 ☐ E-mail/Messaging Software

STORAGE

- 29 ☐ SAN
30 ☐ NAS
31 ☐ Storage Services
32 ☐ Storage Management Software
33 ☐ Disk Drives/Disk Back-up
34 ☐ Tape Drives/Tape Back-up
35 ☐ Optical Storage

SERVERS

- 36 ☐ File/Print Servers
37 ☐ Web/HTTP Servers
38 ☐ Remote Access Servers
39 ☐ Voice Servers/IP PBXs
40 ☐ Video Servers

SECURITY

- 41 ☐ VPN Hardware/Software
42 ☐ VPN Services
43 ☐ Encryption Software/Devices
44 ☐ PKI
45 ☐ Firewalls
46 ☐ Anti-virus Software
47 ☐ Intrusion Detection Software/Devices
48 ☐ Authentication/Single Sign-on

WIRELESS

- 49 ☐ Wireless/Mobile Data Services
50 ☐ Wireless LAN
51 ☐ Fixed Wireless
52 ☐ Mobile Computing Hardware/Software

DIAGNOSTIC/TESTING

- 53 ☐ Cable Testers
54 ☐ Protocol Analyzers
55 ☐ Troubleshooting Tools
56 ☐ RMON/Instrumentation

SERVER OPERATING SYSTEMS

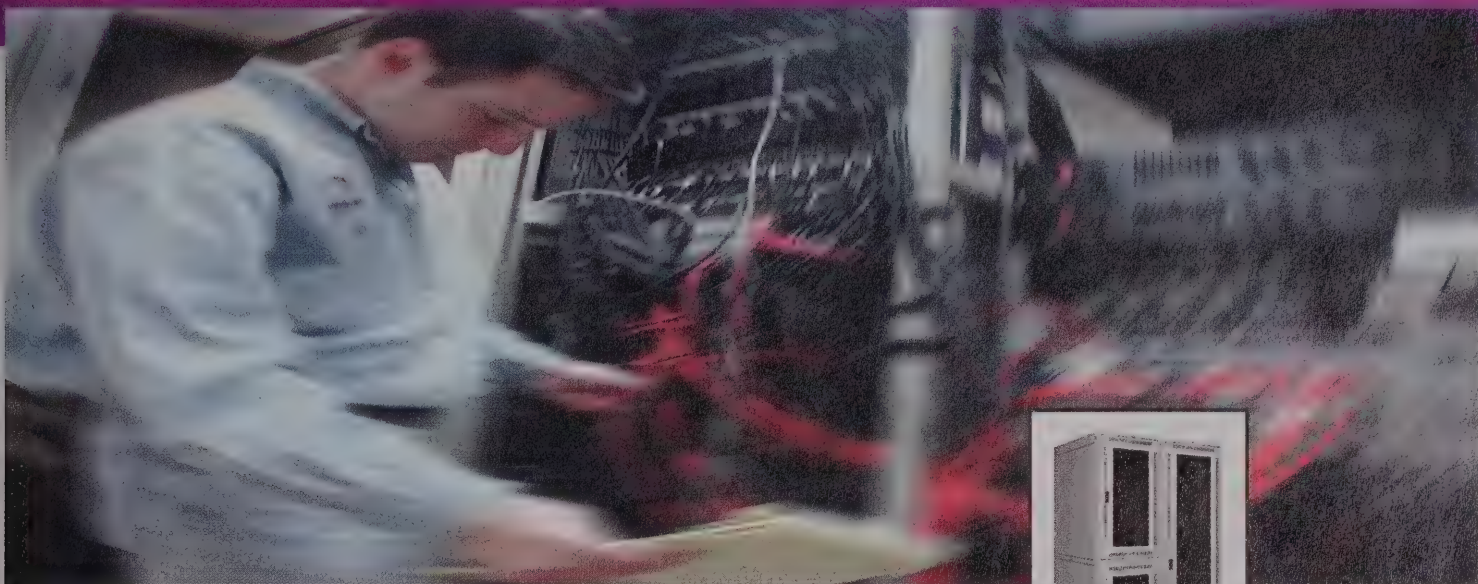
- 57 ☐ Windows NT/2000/XP
58 ☐ NetWare
59 ☐ Linux
60 ☐ Solaris
61 ☐ Unix (HP/UX, AIX, etc.)
99 ☐ None of the Above

7 How large is your organization's network? (If reseller, use your largest client's company): (check one)

- 01 ☐ 100,000 + nodes
02 ☐ 50,001 - 100,000 nodes
03 ☐ 10,001 - 50,000 nodes
04 ☐ 1,001 - 10,000 nodes
05 ☐ 100 - 1,000 nodes
06 ☐ Less than 100 nodes

Thank you for your response

So many servers, hubs, switches, cables...



One Solution.

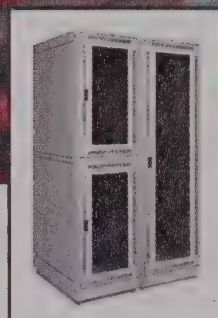
Too much equipment. Not enough space.

We can help.

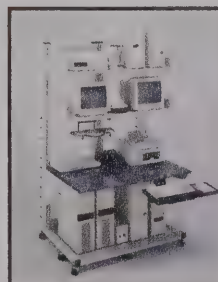
Ergotron optimizes your data center space with exceptional network furniture, enclosures, Avocent KVM technology, diagnostic crash-carts and other innovative products that will make your life easier.

Ergotron is the solution you need in the data center.

Learn more now. Get the entire story at onesolution.ergotron.com.



**Universal
rack-mount
Enclosures**



**Open-frame
modular
Network
furniture**



**Avocent digital
KVM Switches**



**Data center
crash-carts**



Call 1.800.888.8458 (U.S.)
1.800.267.9912 (Canada)



www.buyuptime.com
**BUY
UPTIME**
.com

BuyUptime.com

Your One-Stop Shop for high availability products

Network Cables

Cisco and Fiber
Cabling

Printer, Modem VGA
Cables and Adapters

Enclosures

Enclosure Accessories

Power Adapters

Cooling Solutions

Laptop Accessories

Racks

Rack Accessories

Power Distribution
Devices

Security Hardware

Surge Protectors

UPS Cables and
Accessories

UPS Management
Peripherals

UPS Management
Software

UPS Replacement
Batteries

UPSs

High Availability Made Easy

As a leading supplier in end-to-end UPS power, thermal cooling and management solutions, BuyUptime.com can accommodate the level of availability many customers have come to expect. Join us today and let BuyUptime be your one-stop shop for high availability solutions.



Hot Summer, Cool Network!

NetworkAIR™ 1000

The NetworkAIR 1000 is a portable, compact, air conditioner designed for spot-cooling, emergency cooling and after hours cooling of server closets, data centers, conference rooms, home offices or rooms housing heat-sensitive equipment. Providing 1.6kW of supplemental cooling, the NetworkAIR is a great choice for eliminating localized hot spots.

\$799
(including shipping
and handling)

Part # AP7003

Additional Features Include:

- Electronic control panel with LCD display
- Automatic turn-on/shut-off timer
- Oscillating automatic swing louvers for even air distribution in the room
- Includes ceiling warm air exhaust kit
- Quiet, high efficiency rotary compressor
- Programmable digital thermostat

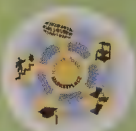
Order via our promo page and save an additional **\$10**

Visit <http://promo.buyuptime.com>

and enter the Key Code f304y

Call Toll Free
888-288-8843 to order.

Fax: (877) 411-2080 • E-mail: customerservice@buyuptime.com
801 Corporate Centre Drive, St. Charles, MO 63304 • BY2A1EP-USd
©2002 Systems Enhancement Corp. All Trademarks are the property of their owners.



Network Magazine
MARKETPLACE

interested in

GENERATING

high
quality

LEADS?

The
Marketplace
Section in
Network
Magazine:

the perfect equa-
tion to reach
200,000 network/
IT buyers.

ACTIVE
readers



POWERFUL
circulation mix



RIGHT
environment



QUALITY
leads

WHAT ADVERTISERS SAY

"Quality leads are hard to find and our experience is Network Magazine delivers them." – Chuck Sheldon, CEO, Network Hardware Resale, LLC

"Network Magazine is one of our best print resources for lead generation." – Kevin Lewis, Marketing Director, LearnKey, Inc.

"Not only do we receive numerous qualified leads on a continuous basis, but the content is interesting, quality, topical and a helpful way to track industry trends." – Karen M. Freeman, Marketing Communications Manager, Western Telematic, Inc.

"Network Magazine provides the right environment to reach our customer and the reward is high quality leads." – Kate Hunt, Associate Marketing Manager, Ergotron, Inc.

For more information on Marketplace section advertising, contact Bethany Baller at 585.342.2484 or bballer@cmp.com.

Server Access Over IP

Moves Remote Server Management to a Higher Level



**CONTROL IT
SECURE IT
MANAGE IT
FROM ANYWHERE**

The UltraLink is the Rose Electronics answer to Modem and Ethernet remote access!

Server access over IP technology allows you to access, control and provide computer maintenance from anywhere in the world. When combined with Rose KVM switch technology, server management administrators can have faster access saving time and money.

With dial-in, dial-back security and high-resolution quad screen and SSL encryption, the UltraLink raises the KVM industry bar in remote server access. A KVM industry pioneer, Rose Electronics is recognized for superior KVM switch technology.

Product integrity, simplicity, and reliability are the hallmarks of all Rose products.

Call Rose to learn more about remote server management today.

ROSE ELECTRONICS
10707 Stancliff Rd.
Houston, Texas 77099
281-933-7673

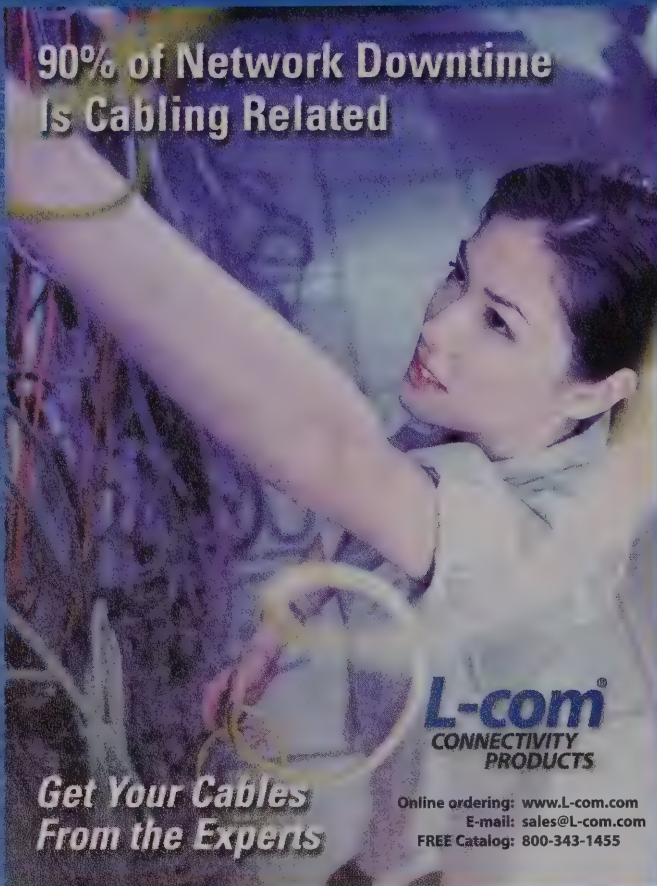
800-333-9343
WWW.ROSE.COM

USA . CANADA . ENGLAND . FRANCE . GERMANY . BENELUX . AUSTRALIA . SINGAPORE

 **ROSE**
ELECTRONICS



90% of Network Downtime
Is Cabling Related



Get Your Cables
From the Experts

L-com
CONNECTIVITY
PRODUCTS

Online ordering: www.L-com.com
E-mail: sales@L-com.com
FREE Catalog: 800-343-1455

WE BUY
AND SELL

**USED
CISCO**

SINCE 1985

800.451.3407

networkhardware.com

new and used
fully guaranteed
overnight delivery

routers
switches
access servers
interface modules
accessories

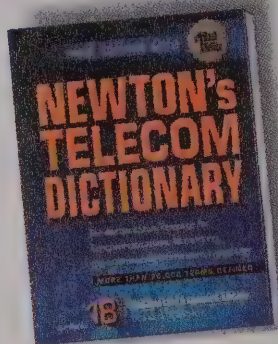
we also buy and sell:

IBM, HP, Dell, Compaq
Sun, Microsoft, Intel
Cisco, 3Com
and other technology

Se habla Español
Wir sprechen Deutsch

NETWORK HARDWARE RESALE

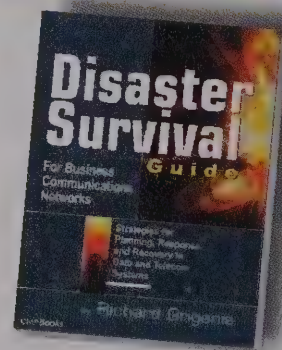
www.cmpbooks.com



Newton's Telecom Dictionary

Keep up with the ever-changing telecom and Internet markets with this industry "bible". With over 20,000 definitions – including intranet, broadband services, wireless and e-commerce terms – this edition is over four times larger than its nearest competitor. Harry Newton uses non-technical language to explain these technical concepts.

ISBN 1-57820-104-7, \$34.95



Disaster Survival Guide for Business Communications Networks

Protect your business from natural and manmade disasters. This book explores strategies and solutions for disaster planning, mitigation, response and recovery for data and telecom systems and networks. Discover which technologies keep your business running and protect your employees from unnecessary risk.

ISBN 1-57820-117-9, \$49.95

Find **CMPBooks** in your local bookstore

800-500-6875 • cmp.rushorder.com

Look for these other great rack accessories from APC:

Fixed and Sliding Shelves
Cable Management Shelves
Fans
Keyboards/Keyboard Drawers
Stabilization Kits
Power Distribution Units

Visit www.apc.com
for more information!

Rack 'Em Up with APC!

APC, the name you trust for power protection, also offers a comprehensive line of non-proprietary racks, rack accessories and management tools that provide you with the flexibility to implement a highly available, multi-vendor environment. APC allows you to create a rack environment with the level of availability you

require and provides you with the accessories and management tools to maintain that level of availability over time. Our expert Configure-to-Order Team can custom tailor a complete rack-mount solution to suit your specific requirements. Contact APC today and protect your rack application with Legendary Reliability™.

Air Distribution Unit

A unique 2U rack-mounted fan tray unit that connects into raised floors and pulls conditioned air directly into the enclosure

- Dual fans provide increased air flow needed to cool densely packed equipment
- Improves air delivery in poor static pressure areas
- Enhances air quality to rack equipment by providing 30% efficient filtration
- Adjustable depth to fit most leading enclosures

NEW!



NetShelter® VX Enclosures

Next generation, high-quality enclosures

- Fully ventilated front and rear doors with enhanced ventilation pattern maximize airflow
- Overhead, base and side cable access provide easy, integrated cable management
- Rear Cabling Channel (42"-deep versions only) allows for easy installation, access and serviceability of both data cables and power distribution
- Available in multiple configurations: 35.5"-deep, 42"-deep, beige or black



NetShelter® Open Frame Racks

Economical open frame solutions for wiring closets and data center networking applications

- Designed to accommodate networking devices such as hubs, routers and switches
- Industry standard 7"-high design provides 45U of equipment mounting space
- Self-squaring design allows one-person assembly
- Made of high-strength 6061-T6, structural-grade aluminum



MasterSwitch™ Series

Remote power distribution for network administrators

- Users can configure the sequence in which power is provided to individual receptacles upon start-up
- Built-in Ethernet interface for direct connection to LAN
- Individually control 8 on-board power outlets for complete and flexible management of attached equipment

APC MasterSwitch™ VM shown mounted inside a NetShelter® VX



KVM Switches

Server switches designed to increase system availability and manageability

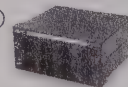
- 4 and 8-port models available: expandable to support up to 64 servers
- Models available that support Sun, USB and PC servers simultaneously
- Built-in scanning feature allows you to automatically monitor your computers without intervention
- On Screen Display (OSD) functionality, advanced security features



ProtectNet®

Data line surge suppressors for comprehensive network/PC system protection

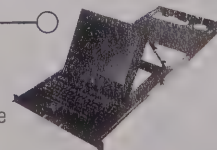
- Protects against surges and electrostatic discharge traveling through data lines



LCD Monitors

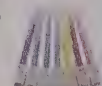
High quality rack-mount LCD monitors designed to maximize space in a data center environment

- Provides optimal functionality while utilizing only 1U (1.75") of rack space
- Includes 15" LCD monitor, integrated keyboard and integrated pointing device



Cables

- APC offers a comprehensive line of cables and connectivity solutions to fulfill the connectivity requirements of any application or environment



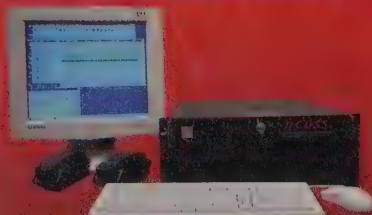
Configure your racks with APC. Simply visit promo.apc.com today!

Key Code f305y • Call 888-289-APCC x6418 • Fax 401-788-2797

APC
Legendary Reliability™



Digital Central Office Switch Simulator



The Digital Central Office Switch Simulator (DCOSS) converts a Pentium PC (portable, tower, rack-mount) into a digital central office switch simulator, PBX and switch, complete with T1, E1, and POTS interfaces. A user-friendly graphical interface (GUI), through which complex switching, signaling, and digital transmission functions are easily controlled, provides the ease of operation and flexibility required from telephony test equipment. DCOSS is ideal for simulating and testing advanced telecom networks and products, including switches, gateways, and transmission systems. The DCOSS can also be used for verifying T1/E1 signaling protocols of new systems.

- Digital T1/E1 Interfaces & Analog/BRI Telephone Interfaces
- R1, MFC-R2, PRI-ISDN, SS7, & SS5 Signaling Protocols
- Digital Switching with Protocol Conversion
- Manual or Bulk Calling (including Scripting Capability)
- Voice Quality Assessment using PAMS, PSQM, & PESQ
- Remote Access Capability (Client/Server) with Support for Windows, Unix, & Linux
- Load Testing using Real-Time Fax Calls, Modem Traffic, & Voice Files

Visit our website to learn more about GL's T1/E1 Analysis and Voice Quality Assessment Solutions.

GL Communications Inc.

Phone: 301-670-4784 Fax: 301-670-9187

E-Mail: info@gl.com Web: www.gl.com/dcoos

Announcing...

The Quickest and Easiest Path To Reduced Costs and a More Efficient Help Desk



• Help Desk • Inventory • Purchasing • LAN Auditing • Training • Reporting • Web • And More!

Track-It! is the complete system for microcomputer management. Why purchase separate systems for managing PC Inventory, LAN Auditing, Purchasing, Help Desk, Training, Reporting, and Web or any of the other functions that Track-It! includes for one low price?

Track-It! reduces your operational costs and gives you the facts you need to make informed decisions. See why Track-It! pays for itself in days!

- Automate the tracking and escalation of your work orders
- Automatically populate your inventory via LAN or diskette
- Tap into the power of the web to expand the functionality of your Help Desk
- Reduce your operational costs and increase your efficiency
- Plus a lot more...

BlueOcean
SOFTWARE INC.

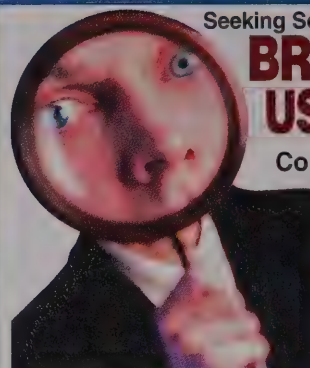


To learn more: call 813-977-4553 and ask for the "NAD Demo" or visit <http://blueocean.com/demo/NAD.html>

"The World's #1 Inventory/Help Desk Management System"

Seeking Solutions ...NTI Has The Answers!

BREAKTHROUGH USB KVM SWITCH



Control from two computers to hundreds of servers - NTI has the innovative KVM solution for you.

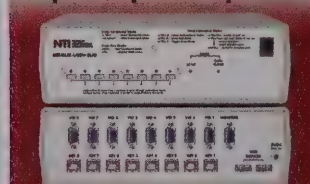
NOW SUPPORTS USB KEYBOARDS AND MICE!

Compatible with USB - enabled PCs, MAC G3/G4, HPJ5000 & other USB - enabled UNIX computers.

Controls up to 32 computers with USB peripheral ports.

Fully compliant with USB standards.

Crisp & clear 1900x1200 resolution.



KEEMUX-USBV-8U0

NEW UNIVERSAL USB SWITCH

BUY ONLINE at www.nti1.com

Phone: 800-742-8324

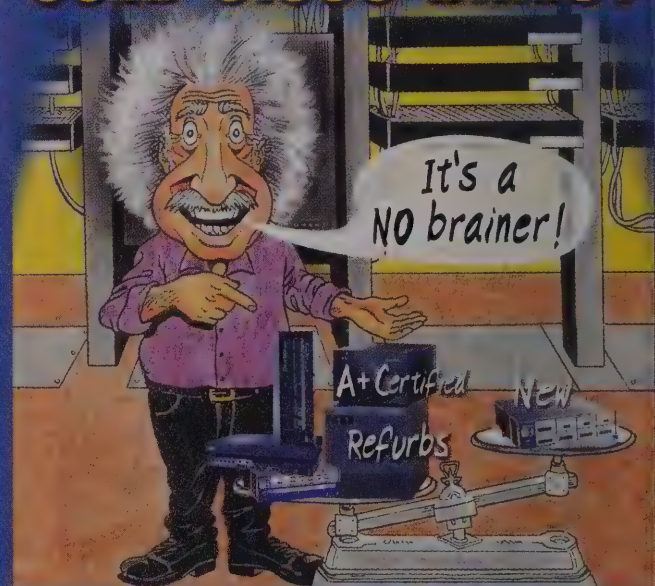
Email: sales@nti1.com



1275 Danner Drive • Aurora, OH 44202
330-562-7070 • FAX: 330-562-1999

KEEMUX KVM SOLUTIONS

USED CISCO DIRECT



Pay Less Get More!



- | | | |
|--|--------------------|-----------------------|
| ■ Cisco Systems | ■ Extreme Networks | ■ Nortel Networks |
| ■ Juniper Networks | ■ Foundry Networks | ■ Lucent Technology |
| www.digitalwarehouse.com | | ■ Alcatel |
| DIGITAL WAREHOUSE | | ■ Riverstone Networks |

Your Information Superhighway Discount Source®

Phone: **800-439-8558** or **718-894-7500**
56-29 56th Drive, Massapequa, NY 11378 USA • Fax: 718-894-1572

got cat 6?

ELITE

ELITE

- Plenum
- Connectors
- Patch Cords
- Patch Panels
- Fiber

Your Source for
Tomorrow's Network
Today!

ABA Industry, Inc.
(888) 534-7776

www.aba-industry.com

"This is the way to learn!"

"I loved the instruction. The tests, the labs and other tools all contribute to a great learning experience and the instructor was with me all the way. I knew I was prepared for certification and thanks to LearnKey, I passed!"

LearnKey training for

IT CERTIFICATION



Special savings* on these great titles:

Win 2000 MCSA Core Series	15 Sessions	\$ 795	reg. \$1,085
Win 2000 MCSA Plus Series (with A+ & Network+)	27 Sessions	\$ 1,445	reg. \$1,925
Windows 2000 Core Series	19 Sessions	\$ 995	reg. \$1,355
Windows XP Professional	6 Sessions	\$ 370	reg. \$ 495
Cisco® CCNA Course	5 Sessions	\$ 370	reg. \$ 495
ASP.NET For Developers series	13 Sessions	\$ 835	reg. \$1,115
A+ Certification Course	8 Sessions	\$ 475	reg. \$ 635



**Windows XP
Professional**

6 Sessions

\$370*

reg. \$495



**ASP.NET
For Developers Part 1**

6 Sessions

\$435*

reg. \$585



**A+
Certification**

8 Sessions

\$475*

reg. \$635



**Cisco® CCNA™
Training**

5 Sessions

\$370*

reg. \$495

Ask about our Exam Bundles with test prep, study guides and mentoring!

Available ONLY at learnkey.com/netmag

NETWORK • ONLINE • CD-ROM • VIDEO

Microsoft® • CompTIA® • Novell® • Cisco® • CIW®

1.800.865.0165 • learnkey.com/netmag

© 2002 LearnKey, Inc. LK040402

*Limited time offer, some restrictions. Prices listed are for Single-Users. Please call for Multi-User pricing and Corporate solutions



Learn From
The Experts™

Source Code #4105



HARDWARE



CAREERS

MPLS-based services are exploding, but they're not always what they seem.

Is Frame Forwarding the Next Service Sensation?

by Tom Nolle

In the good old days, networks were deployed on a per-service basis. Want frame relay? Buy a frame switch. Today, the rage is multiservice networking, and no technology in this space is hotter than Multiprotocol Label Switching (MPLS). All the big facility carriers are looking to make major MPLS commitments in 2002, so users can expect to see familiar services such as frame relay offered on unfamiliar network platforms—and at attractive prices. But don't expect them to work like they did in the good old days.

Like frame relay and ATM virtual circuits, MPLS label-switched paths (LSPs) resemble virtual wires. But the IETF's requirements for LSPs are quite different from the aforementioned protocols—so different that services based on MPLS LSPs should be given a completely different name, such as “frame forwarding.” Some carriers are thinking about doing just that to alert users to very real problems that can be created when protocols designed for the virtual circuit frame/ATM world are used with any IP tunnel—including MPLS.

THE REAL THING?

A virtual circuit follows a fixed path in the network. Resources along that path can be guaranteed, making QoS controllable. When packets flow along the route, they stay in sequence, and if the route is disrupted, notification is quickly sent to the endpoints telling them that the path is lost. Somewhere between a fifth and a quarter of frame relay traffic today is dependent on one or more of these characteristics. The majority, however, ignores the detailed frame relay standards and specifications. The popular “zero Committed Information Rate (CIR)” frame relay service, for example, has no more QoS guarantees than an IP network's tunnel service, which isn't much.

When an IP tunnel, or even an MPLS LSP, carries traffic to the resource, guarantees are less stringent and the path is subject to rerouting if network topology changes. Packets can get out of order and, if the path is lost, it might be a half-minute before the loss is reported to the

applications—if it's reported at all. In short, MPLS isn't a real substitute for frame relay or ATM virtual circuits.

This doesn't mean that “frame forwarding” isn't a good idea, though. Because MPLS-based networks are good at supporting new IP-based network services, they offer a lower risk of obsolescence. Many also believe that IP operations costs are lower, which translates to lower service cost for users.

Nomenclature may be the biggest risk. Some MPLS vendors assert that they can provide frame relay-like performance over MPLS LSPs. Others offer MPLS-based services that they call “frame relay.” To complicate things further, some frame forwarding services may work fine with current frame relay applications! What's a user to do?

First, find out whether any new “frame relay” offering really adheres to the full standard, including in-order arrival of packets and fast notification of network problems. In particular, look at whether the carrier will guarantee in-order arrival of packets. Get this guarantee in writing! If the carrier won't provide a guarantee, it's a sure bet that the service is really a frame forwarding service.

Second, determine if you're running applications other than IP. Are your frame relay connections linked to IP routers only, or do you have specialized Frame Relay Access Devices (FRADs)? Do you do LAN bridging, or run IBM's SNA protocol? Are you running old LAN resource-sharing protocols in addition to IP? If the answer to any of these questions is “Yes,” you might be facing major application failure if you try to run your traffic over a frame forwarding service connection.

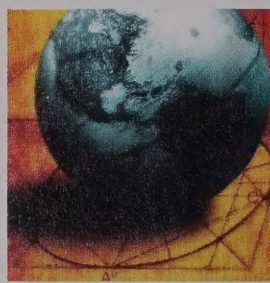
Third, check with your equipment vendor to see if your current devices will allow a frame relay interface to be used without the specific features called out in

the standard. For example, most frame forwarding services won't offer explicit congestion notification features, so if your hardware depends on those features, there may be network stability problems. On the other hand, most users disable these congestion management features, so don't dismiss a service just because congestion management isn't supported. The carrier offering frame forwarding services may provide a list of compatible equipment, and even tell you how to set up the equipment for optimal performance and stability.

Finally, check your own procedures for introducing new applications, particularly if you're converting from “true” frame relay to frame forwarding. Many companies let users run nearly anything they want on the LAN, and if a new application depends on features such as in-order packet delivery, it may fail when the frame forwarding service gets packets out of order.

What you should *not* do is try to test or monitor your network to see if you're running applications sensitive to the frame forwarding service's differences. While some users have reported failures daily with frame-over-MPLS services, most won't see symptoms of problems regularly enough to test.

The use of MPLS devices inside carrier networks will explode around mid-2002. This will result in the deployment of many frame relay-like services that may or may not actually duplicate all the features of the standard service. The price advantages of these new services may be significant, but be sure they'll work with your present and future applications before you make a commitment. *

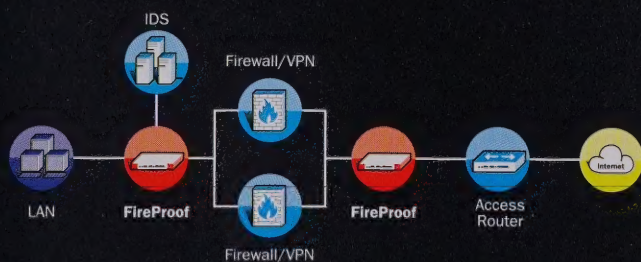


MPLS isn't a real substitute for frame relay or ATM virtual circuits.

Tom Nolle is president of CIMI (www.cimi-corp.com), a consulting firm for strategic technology planning. He can be reached at tnolle@cimicorp.com.



FireProof Security Application Switch: Enterprise Wide Security with Assurance



FireProof is the industry's first security Application Switch that ensures the integrity and operation of your security infrastructure across the enterprise. Combining load balancing, optimization and high availability for firewalls, VPNs and IDS devices, FireProof eliminates bottlenecks and single points of failure, guaranteeing full availability, operation and optimized security devices. FireProof's DoS Shield module prevents DoS attacks, while maintaining high throughput on users' networks. An additional layer of defense is delivered through our award winning application security module, preventing more than 450 attack signatures.

Choose FireProof for robust enterprise security.





MAYBE "CUSTOMER SERVICE" SHOULD BE MORE THAN ONE DEPARTMENT.

When everyone focuses on customers, something amazing happens: departments communicate, questions get answered, and products keep moving. That's why the mySAP™ Customer Relationship Management solution links customers with your complete organization. It keeps data consistent across all touch points and it's the only CRM solution that integrates with all other business processes, so it shortens sales cycles and lowers costs. Which means your customers won't be waiting around for good service, they'll be too busy getting it. For more info, visit www.sap.com

THE BEST-RUN E-BUSINESSES RUN SAP

